A GAME-THEORETIC APPROACH TO THE SECURITY OF EMERGING COGNITIVE RADIO AND SMALL CELL NETWORKS

BY

ALI KAMAL HOUJEIJ

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2013

Urbana, Illinois

Adviser:

Professor Tamer Başar

ABSTRACT

In this thesis, we provide mathematical formulations for and investigate a number of problems that arise in the security of some emerging wireless technologies. First, we address the problem of secure communication between secondary users (SUs) and their serving base station in the presence of multiple eavesdroppers and multiple primary users (PUs) in cognitive radio networks. We analyze the interactions between the SUs and eavesdroppers using the framework of noncooperative game theory. Assuming that the SUs have full knowledge of the eavesdroppers, we propose a novel secure channel selection algorithm that enables the SUs and eavesdroppers to take distributed decisions so as to reach a Nash equilibrium point. Then, we solve the same problem using a different approach and under a different set of assumptions. Here, the SUs aim at mitigating the effect of eavesdropping by changing their positions using only partial information about the locations of the eavesdroppers. Accordingly, for each SU, we propose an appropriate utility function and then maximize the social welfare of all SUs without interfering with the PUs' radio receivers and taking into account the interference thresholds set by the PUs on each channel. Given these constraints, we formulate the problem so as to optimize the social welfare of all SUs and we present three different algorithms to solve the emerging constrained optimization problem, depending on the possible communication links and the available information. Finally, we investigate the problem of placing small cell base stations (SCBSs) in adversarial heterogeneous wireless networks. We consider a continuum of wireless users facing three types of attacks: eavesdropping, jamming and a combination of both. For each attack, we propose a suitable utility function for the wireless users. Then, we propose a novel optimal placement algorithm for finding the optimal locations of the SCBSs given the underlying security considerations. Simulations were carried out for all the proposed algorithms.

To my lovely parents, sisters, and brother: for their care, trust, support, and love.

ACKNOWLEDGMENTS

I am deeply grateful to my adviser, Prof. Tamer Başar, whose guidance, patience, and academic experience were the keys for the accomplishment of this thesis. Our weekly meetings deepened my understandings of control and game theory and helped me acquire new insights and research ideas.

I would like to thank Dr. Walid Saad for providing me with his research and technical experiences throughout the past two years. His deep knowledge of networks and communications helped me solve my research problems.

I would like to acknowledge AFOSR MURI Grant FA9550-10-1-0573, and Boeing and NSA through the Information Trust Institute at the University of Illinois for the full support during my master's degree. Also, I would like to thank the U.S. National Science Foundation under Grant CNS-1253731.

I am very thankful to my research group, mainly, Ali, Rasoul, Abhishek, Jun, and Bahman for being excellent company and for the important discussions that helped me overcome the different problems I faced during my research. My friends at UIUC were a constant support and, whenever needed, a great source of motivation. To my friends in Lebanon, Thank you for being there for me and for making my life away from home much easier.

I am deeply grateful to my family, who were always loving and supportive. Mom, Dad, Faten, Fatima, and Abduallah, I couldn't have done much without you all. May God grant me the health and strength to honor you throughout my life.

Finally, and most importantly, I thank God, the Most Gracious, the Most Merciful.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Security in Emerging Wireless Technologies

The demand for wireless services has grown exponentially in the past decade and is expected to continue to do so in the foreseeable future [1]. This growth was accompanied by an increase in the number of wireless users and higher traffic rates, thus straining the current wireless cellular system. To address these challenges, researchers have been developing new paradigms in network design. Hence, emerging wireless technologies, such as cognitive radio (CR) and small cell networks, were introduced to boost the efficiency and spatial utilization of the radio spectrum [2–7].

The increase in mobile traffic, the broadcast nature of the wireless medium and the sensitivity of the data being sent render the wireless network vulnerable to security attacks. According to recent studies, more wireless mobile users were targeted over the past few years causing security concerns and service outages [8]. These increasing threats have caught the attention of service providers, who are recently introducing new security measures to target these problems [8].

Accordingly, it is of paramount importance to address the security aspects of the emerging wireless technologies. But, with the evolution of mobile and decentralized networks, implementing traditional cryptographic techniques over large-scale wireless systems is becoming an increasingly complex task due to the associated computational overhead, especially in a resource constrained environment. Recently, physical layer (PHY) security has emerged as a promising solution for securing communication over the wireless medium. PHY security was first introduced in Wyner's seminal work [9] over the wire-tap channel and it was then extended to wireless and multi-user channels [10–12]. The main idea behind PHY security is to exploit the wireless

channel characteristics, such as noise and fading, so as to improve the reliability of wireless transmission. This reliability is quantified through the notion of *secrecy rate*, which is defined as the rate of secret information sent from a node to its destination without being tapped in by malicious eavesdroppers.

1.2 Cognitive Radio Networks

The use of PHY security is of great importance for emerging cognitive radio networks. In a CR network, a number of distributed, often ad hoc, unlicensed secondary users (SUs) are able to transmit over the licensed radio spectrum, when the associated channels are not being utilized by licensed primary users (PUs) [3]. The decentralized nature of CR networks and the increasing volume of wireless attacks and attackers introduce numerous security threats to the communicating SUs [13–17]. For example, the authors in [13] discuss how the SUs can help increase the secrecy of the PU transmissions by appropriately choosing the channels and power levels. They model the interactions between the SUs and PUs as a Stackelberg game. The authors in [14] investigate denial-of-service attacks against CR networks and introduce a few potential protection remedies. In [15], a study of primary user emulation attacks is presented. The authors analyze the equilibrium of a game between malicious and legitimate SUs. Another type of attack was considered in [16] where the authors address the problem of compromised SUs reporting false spectrum sensing results. The authors provide a solution technique to detect malicious SUs by assigning suspicious levels to each node. A comprehensive survey of CR attacks and countermeasures is presented in [17].

One important aspect of CR is spectrum sharing whereby SUs must choose their preferred channel for access depending on the tradeoff between channel availability and the mutual interference resulting from the choices of other SUs. The problem of spectrum sharing was extensively studied in the literature [18–20]. For example, the authors in [18] propose a cooperative game for distributed spectrum sharing, while the authors in [19] propose a noncooperative solution for dynamic spectrum access. A list of spectrum sharing techniques is given in [20].

As the SUs are utilizing the CR network to transmit more sensitive and

important data, the presence of active or passive threats constitutes a major concern for SUs, affecting their decision making process. Despite the wealth of existing works on security in cognitive radio networks [17], little has been done to address how the potential presence of eavesdroppers and the quality-of-service demands of the PUs can affect the choices of the SUs. In particular, in this thesis, we will first analyze how the SUs' need to optimize their secrecy rates, in the presence of eavesdroppers, affects the spectrum sharing process. This becomes more challenging when addressing both the spectrum sharing and the security aspects of the problem. In that case, the SUs must observe various parameters such as PUs' activity, mutual interference, and any potential or suspected eavesdropping, before choosing the transmission channel. Here, we assume that the SUs have complete knowledge of the eavesdroppers. Secondly, we will consider the case of mobile SUs who need to ensure a fast and secure communication link with the base station (BS) in the presence of eavesdroppers. By changing their positions before transmission, the SUs aim at mitigating the effect of potential eavesdropping using only partial information about the positions of eavesdroppers. To our knowledge, no previous work seems to have investigated how this potential presence of eavesdroppers can impact the channel selection and movement strategies of the SUs in a cognitive network.

1.3 Small Cell Networks

Another propitious emerging wireless technology is small cell networks. Small cell networks, also known as heterogeneous networks, are seen as a promising solution for the growing demand in mobile cellular systems. Small cells are based on the deployment of low power, low cost, small cell base stations that are overlaid over cellular networks. There are multiple types of small cells, each having its unique set of features that identifies its role in the network. On the one hand, femtocells are small, user-deployed indoor access points used to provide extra coverage in houses or small businesses. On the other hand, picocells and microcells are larger, operator-deployed outdoor stations used by network operators to boost network capacity in high traffic areas. Small cells are becoming very popular, and according to recent reports, over six million small cells were deployed by the end of 2012 [21]. This surpasses

the overall number of deployed macrocells at 5.9 million worldwide. The market forecast also predicts that, by the end of 2016, there will be around 91 million small cells deployed globally [21].

For the operator-deployed picocells and microcells, optimally placing the small cell base stations (SCBSs) is vital to reap the benefits of small cell networks. Indeed, deploying SCBSs so as to optimize the overall quality-of-service of the wireless users is a key problem. Remarkably, little work seems to have investigated the network planning problem in the presence of small cells. Most of the existing network planning works have been focused on the deployment of conventional macro-cellular base stations [22–25]. For example, the authors in [24] consider the problem of optimally placing two base stations on a line to maximize the signal to interference plus noise ratio (SINR) of wireless users. The authors study the hierarchical equilibrium to conclude the optimal placement of base stations. The work was limited to the study of two base stations on the real line. The authors in [25] address the problem of heterogeneous base station deployment. They study how deploying additional SCBSs into existing networks can boost the energy efficiency of traditional macrocell deployment.

Particularly, as small cells can be massively deployed and practically anywhere, their transmission becomes more susceptible to security threats. The broadcast nature of the wireless medium renders heterogeneous networks vulnerable to different types of attacks. To address such threats, the authors in [26] consider the problem of the secure placement of relays in general wireless networks under eavesdropping attacks. Using physical layer security techniques, the authors formulate the problem with a single sender and a single receiver without the relay. The relay is then optimally placed in the network to maximize the secrecy rate of users. The work in [27] takes a different approach to evade jammers in heterogeneous mobile networks. The problem is formulated as a zero-sum pursuit-evasion game and its saddle point equilibrium is studied.

Non-secure SCBS deployment techniques do not account for potential security threats in the network. These techniques will provide the attackers with better network resources and may end up favoring them over the wireless users. Therefore, accounting for potential attacks before placing the SCBSs improves the security of the network. The work in [24] can be used to optimally place small cells, but it only considers two base stations, is restricted

to a linear system, and does not account for potential security threats. Also, the works in [26, 27] can be helpful in targeting jamming and eavesdropping attacks in heterogeneous networks, but they do not treat the deployment problem. In this thesis, we consider the problem of optimally placing SCBSs given underlying security considerations. This problem is particularly challenging as the placement of SCBSs has to accommodate both the quality of user channels and the potential security threats at different points in the network. In addition, the placement problem has to change the techniques used in order to accommodate each potential threat.

To this end, we focus on two key physical layer attacks on small cell networks: eavesdropping and jamming, as they constitute a major threat in next-generation decentralized heterogeneous systems [28–31]. For example, such security threats are common in military networks, in which the deployment of small cells can boost the network's efficiency. Due to the confidentiality and importance of the military data being transmitted, accounting for potential jamming and eavesdropping threats should be considered when placing the SCBSs or other similar wireless access points. Also, as mobile payment systems are becoming popular, more sensitive and secure data is being sent from mobile devices very frequently. Accordingly, protection against eavesdropping in mobile communication is of central importance. In addition, the proliferation of denial of service and jamming attacks coupled with the need for providing higher wireless data rates implies that the protection of wireless transmission against jamming is of paramount importance. To our knowledge, no previous work seems to have investigated how this potential presence of eavesdroppers and jammers can affect the placement of SCBSs in a heterogeneous network.

1.4 Main Contributions

The main contribution of this thesis is to address how the potential presence of security threats affects the design of emerging cognitive radio and small cell networks. In particular, we start by looking at a CR network being attacked by a set of eavesdroppers. Each of these eavesdroppers can only wiretap one channel at a time. In this scenario, we introduce a novel scheme which enables the SUs to strategically decide on their preferred secure communica-

tion channel, given complete knowledge of the eavesdroppers. To this end, we formulate a noncooperative game between the SUs and the eavesdroppers. This game consists of two levels of competition. On the one hand, the SUs need to choose their preferred channel so as to optimize the tradeoff between interference (due to channel congestion), availability (due to PUs' activity) and secrecy rate (due to the potential of being eavesdropped). On the other hand, the eavesdroppers are strategic and need to choose the channels that enable them to minimize the overall network's secrecy rate. We first study several properties of this game and characterize the resulting equilibrium. Then, we propose a distributed, low-complexity learning algorithm that can be adopted by the SUs and the eavesdroppers so as to reach an equilibrium of the game. Using simulations, we evaluate the performance of our algorithm and show that it yields significant performance improvements, in terms of the average secrecy rate per SU, compared to classical schemes.

Secondly, we consider a more complex eavesdropping model. We assume that eavesdroppers are spread over a set of areas and they can simultaneously eavesdrop on all channels in a CR network. In this scenario, we introduce a novel approach that enables the SUs to evade potential eavesdroppers without knowing their exact locations. To this end, we develop a novel model that accounts for eavesdropping while protecting the PU receiver radio from SU transmissions and accommodating for the interference thresholds set by the PUs on each channel. In particular, we study the problem of how mobile SUs can change their positions before sending their messages in order to boost the secrecy of their transmission link. To solve this problem, we first propose an appropriate utility function that incorporates the key aspects of the system such as secrecy, movement costs, and time delay. Then, we propose algorithms to solve the problem in three different scenarios. In the first scenario, the BS has all the information about the SU utilities. Here, we cast the problem as a general assignment problem (GAP) and study its solution. In the second scenario, the BS does not possess the information about SUs. Here, the communicating SUs use a distributed game theoretic approach to arrive at the solution. In the third scenario, we consider the case in which the BS has no information about SUs and the SUs are unable to communicate with one another. Here, we introduce a Lagrangian heuristic algorithm to find the solution. Extensive simulation results are run to assess the performance of the proposed approaches. These results show that the proposed

decentralized algorithms were able to achieve near-optimal performances.

Finally, we look at how the operator of a small cell network can choose the locations of SCBSs in order to boost the performance and secrecy of the user transmissions in the presence of security threats. Particularly, we study the problem of optimally placing SCBSs while jointly addressing three key security considerations: (a) eavesdropping, (b) jamming, and (c) a combination of both attacks. For each case, we propose a novel small cell base station placement algorithm that optimally places the SCBSs so as to optimize the overall performance and reliability of the users' wireless transmission as captured by both quality-of-service and security considerations. For each attack, we study and analyze the network structure, develop suitable utility functions, formulate the secure placement problem, and finally solve it using the proposed optimal placement algorithm. We then simulate the proposed algorithms for different network structures, and compare the obtained results with non-secure placement techniques. Simulation results show that the proposed approaches can mitigate the effect of potential security threats and enhance the performance of wireless users for all the considered attacks.

The rest of the thesis is organized as follows: Chapters 2 and 3 discuss the security of SU transmissions in adversarial CR networks with complete and partial knowledge of eavesdroppers, respectively. Chapter 4 discusses the optimal deployment of wireless SCBSs with security considerations. Finally, conclusions and future works are drawn in Chapter 5.

CHAPTER 2

CR NETWORK SECURITY: PERFECT KNOWLEDGE

In this chapter, we discuss the interactions between the SUs in CR networks in the presence of potential eavesdropping threats [32].

Here, we consider that the locations of both SUs and eavesdroppers are known for all the others in the network. This is commonly assumed in most physical layer security related literature such as in [10, 11] and the references therein. In practice, this can be used to model a variety of scenarios. For example, this could correspond to a case in which SUs suspect the presence of eavesdroppers at a specific predetermined location (such as in the case of a battlefield). This model is also applicable to a network in which the eavesdroppers are not malicious, but rather are legitimate SUs. In such a case, the studied model applies to situations in which some messages are not intended for all nodes of the network, such as when some content is "premium" and should be received only by those who have paid for it (legitimate receivers) while others (eavesdroppers) should be denied access. Generally, it is always possible for eavesdroppers to approximate the locations of SUs by sensing the power of the received signals [33].

To this end, we formulate a noncooperative game between the SUs and the eavesdroppers and study its solutions. This chapter is organized as follows: in Section 2.1, we introduce the system model and describe the game formulation, and in Section 2.2, we provide the proposed game solution. Simulation results are then analyzed in Section 2.3.

2.1 System Model and Game Formulation

2.1.1 System Model

Consider a cognitive radio network composed of a set $\mathcal{M}$ of M licensed PUs or channels which can be accessed by a set $\mathcal{N}$ of N unlicensed SUs, when they are not used for PU transmission. The objective of each SU is to communicate with a common BS by using one of the available PU channels. To model the activity of the primary users, we assume that each channel $m \in \mathcal{M}$ has a probability θ_m of being available, i.e., not being used by its corresponding PU.

We consider a frequency selective Rayleigh fading channel such that the channel gain experienced by SU i on channel $m \in \mathcal{M}$ at the BS is given by $h_{i,m} = \kappa \alpha_m d_i^{-\mu}$. Here, μ and κ denote the path loss exponent and the path loss constant, respectively. The term α_m represents the Rayleigh fading amplitude on channel m, while d_i represents the distance between SU i and the BS. In this chapter, we consider a slowly varying channel with a long coherence time.

In essence, the SUs are interested in choosing the channel that provides the highest transmission rate. Since SUs share the available spectrum, mutual interference occurs when more than one SU chooses the same channel. The SINR perceived by an SU i when transmitting over a channel m is:

$$\gamma_{i,m} = \frac{h_{i,m} P_{i,m}}{\sigma^2 + \sum\limits_{j \in \mathcal{N}_m \setminus \{i\}} h_{j,m} P_{j,m}}, \tag{2.1}$$

where $P_{i,m}$ is the maximum transmit power of SU i on channel m, σ^2 is the variance of the Gaussian noise, and $\mathcal{N}_m$ is the set of SUs that are using channel m for transmission.

The capacity achieved by an SU i over an available channel m is thus given by:

$$C_i^m = \log(1 + \gamma_{i,m}), \tag{2.2}$$

where $\gamma_{i,m}$ is the SINR achieved by SU i on channel m as per (2.1). The capacity C_i^m is set to zero if the channel m is not available.

In this model, each SU chooses the channel which optimizes its capacity at the BS. Now, consider that a set $\mathcal{K}$ of K eavesdroppers is present in the net-

work. Here, we consider practical, inexpensive eavesdropping devices which often have limited hardware and can only eavesdrop on a limited number of channels as discussed in [34–36]. We consider in this chapter the case in which an eavesdropper chooses only one channel at a time to eavesdrop on. In the presence of eavesdroppers, the SUs aim not only to maximize their capacity, but also to choose a channel that can potentially lead to secure communication. To this end, each SU will choose the available channel which can yield the highest *secrecy* rate. This leads to a competitive environment between the SUs, as well as between SUs and eavesdroppers. On the one hand, SUs compete to gain access to the available channels in order to maximize their secrecy rates. On the other hand, the objective of the eavesdroppers is to reduce the secrecy rate of the overall network, or a subset of SUs which they are interested in, by choosing their optimal channels. Here, we consider the case in which eavesdroppers want to reduce the overall social welfare of the network. Certainly, our approach can also accommodate other eavesdropping models. For example, with some minor changes, one can also consider adjunct cases such as the one in which the eavesdropper attempts to minimize the secrecy of a certain selected SU (e.g., the weakest).

Given a set $\mathcal{K}_m$ of eavesdroppers active on a channel m, the secrecy rate achieved by an SU i is given by:

$$\tilde{C}_i^m = \left(C_i^m - \max_{k \in \mathcal{K}_m} C_{i,k}^m \right)^+, \tag{2.3}$$

where $a^+ := \max(a, 0)$ and C_i^m is given by (2.2). $C_{i,k}^m$ is the capacity of channel m between SU i and eavesdropper k as received by k and is given by:

$$C_{i,k}^m = \log \left(1 + \frac{g_{i,k,m} P_{i,m}}{\sigma^2 + \sum\limits_{j \in \mathcal{N}_m \setminus \{i\}} g_{j,k,m} P_{j,m}} \right), \tag{2.4}$$

where $g_{i,k,m} = \kappa \alpha_m d_{i,k}^{-\mu}$ represents the channel gain between SU i and any eavesdropper $k \in \mathcal{K}$ where $d_{i,k}$ is the distance between i and k.

It is clear from (2.3) that both channel congestion and eavesdropping decrease the overall secrecy rate of secondary users. Consequently, when an SU tries to maximize its secrecy rate in the presence of multiple eavesdroppers, there is an obvious tradeoff between choosing a crowded channel with better

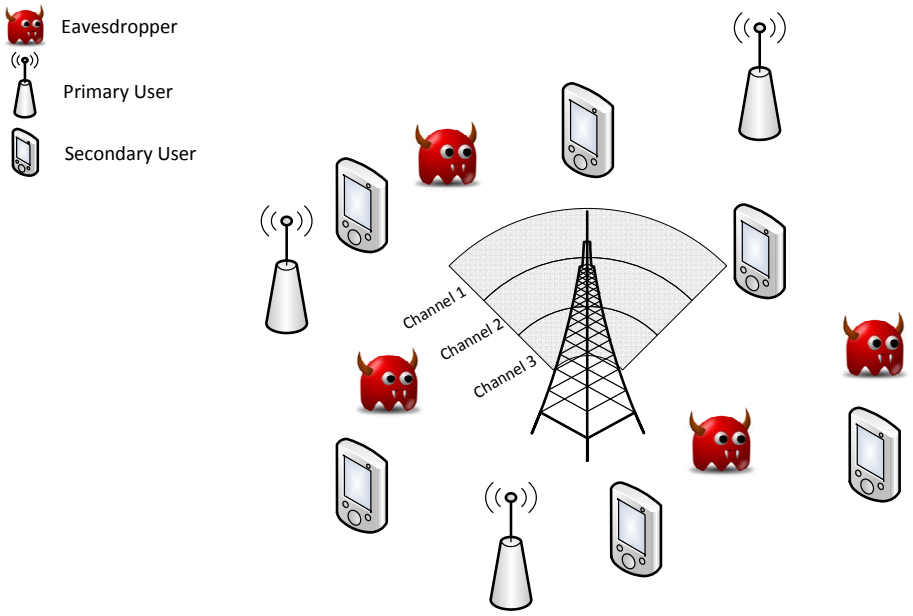

Figure 2.1: A typical system with $N = 6$ SUs and $K = 4$ eavesdroppers and $M = 3$ channels.

secrecy versus a less crowded one with more damaging eavesdroppers. Figure 2.1 shows a typical system in which the SUs and eavesdroppers interact in a CR network with three channels in the presence of four eavesdroppers.

2.1.2 Game Formulation

We use the framework of noncooperative game theory to study the interactions between SUs and eavesdroppers [37]. This problem is game theoretic by nature since both SUs and eavesdroppers want to selfishly maximize their gains.

Denote by $\mathcal{P} = \mathcal{N} \bigcup \mathcal{K}$ the set of all players in this game, that is the set of SUs and eavesdroppers in the network. Players in $\mathcal{P}$ choose their actions from the same action space $\mathcal{M}_i = \mathcal{M}\ \forall i \in \mathcal{P}$ of size M representing the channels in the system. The action $m_i \in \mathcal{M}_i$ of an SU i represents the channel it chooses to transmit on, while the action $e_k \in \mathcal{M}_k$ of an eavesdropper k represents the channel it chooses to listen on. In this section, we define the capacities as functions of the channels, i.e., $C_i(m) := C_i^m$, $C_{i,k}(m) := C_{i,k}^m$ and $\tilde{C}_i(m) := \tilde{C}_i^m$.

We define the utility of the secondary users as the expected value, with

respect to the PUs' activity, of the achieved secrecy rate, expressed in (2.3), when choosing a certain channel. Formally, the utility of an SU $i \in \mathcal{N}$ that selects an action $m_i \in \mathcal{M}_i$ is given by:

$$\begin{aligned}\phi(m_i, \boldsymbol{m}_{-i}, \boldsymbol{e}) &= \mathbb{E}\left[\tilde{C}_i(m_i)\right], \\ &= \theta_{m_i}\left(C_i(m_i) - \max_{\{k \in \mathcal{K}: e_k = m_i\}} C_{i,k}(m_i)\right)^+. \end{aligned} \tag{2.5}$$

Here, $\boldsymbol{m}_{-i}$ represents the vector of all actions taken by all other SUs in the set $\mathcal{N} \setminus \{i\}$, and $\boldsymbol{e}$ represents the vector of actions taken by all eavesdroppers in $\mathcal{K}$. Each SU aims at maximizing its achieved secrecy rate by choosing the channel that maximizes its utility function.

The utility of each eavesdropper is captured by its ability to decrease the secrecy rates of the SUs. Formally, the utility of an eavesdropper $k \in \mathcal{K}$ that chooses an action $e_k \in \mathcal{M}_k$ is given by the expected value, with respect to the PUs' activity, of its eavesdropping effect on all SUs transmitting on channel e_k. Using (2.4), the utility is given by:

$$\psi(e_k, \boldsymbol{m}) = \theta_{e_k}\left(\sum_{i \in \mathcal{N}: e_k = m_k} C_{i,k}(e_k)\right). \tag{2.6}$$

Here, $\boldsymbol{m}$ represents the vector of actions taken by all SUs in $\mathcal{N}$. Clearly, the eavesdroppers are mainly competing with the SUs, but not with one another. Each eavesdropper aims at maximizing its utility in order to increase the damage that it inflicts on the SUs.

Generally, let $a_i \in \mathcal{M}_i$ be the action of player $i \in \mathcal{P}$, i.e., $a_i = m_i$ if $i \in \mathcal{N}$ and $a_i = e_i$ if $i \in \mathcal{K}$. Let $\boldsymbol{a}_{-i}$ be the vector of actions taken by all players in the set $\mathcal{P} \setminus \{i\}$. Given the SUs' and eavesdroppers' utilities as expressed by (2.5) and (2.6), respectively, we define the general utility function as follows:

$$U_i(a_i, \boldsymbol{a}_{-i}) = \begin{cases} \phi(m_i, m_{-i}, \boldsymbol{e}) & \text{if } i \in \mathcal{N} \\ \psi(e_i, \boldsymbol{m}) & \text{if } i \in \mathcal{K} \end{cases} \tag{2.7}$$

Now, let $\boldsymbol{p}_i = \left[p_i^1, p_i^2, \cdots, p_i^M\right] \in \Lambda_i$ be the mixed strategy of player i $\forall i \in \mathcal{P}$. Each component p_i^m can be viewed as the frequency with which player i transmits on channel m, if $i \in \mathcal{N}$, or eavesdrops on channel m, if $i \in \mathcal{K}$. In other words, $p_i^m := \Pr(a_i = m)$. Λ_i represents the space of all possible mixed

strategies for player i and it is defined as $\Lambda_i := \left\{\boldsymbol{p}_i \in [0,1]^M | \sum_{m\in\mathcal{M}_i} p_i^m = 1\right\}$. Let $\boldsymbol{p} = \{\boldsymbol{p}_i,\ i \in \mathcal{P}\}$; then, the expected utility of player i is given by

$$\bar{U}_i(\boldsymbol{p}_i, \boldsymbol{p}_{-\boldsymbol{i}}) = \mathbb{E}_{\boldsymbol{p}}[U_i(a_i, \boldsymbol{a}_{-i})]$$

$$= \sum_{a_1\in\mathcal{M}_1} \cdots \sum_{a_{N+K}\in\mathcal{M}_{N+K}} U_i(a_1, \cdots, a_{N+K}) \prod_{j=1}^{N+K} p_j^{a_j}, \tag{2.8}$$

where $\boldsymbol{p}_{-i}$ represents the vector of mixed strategies of all other players in $\mathcal{P} \setminus \{i\}$.

We now formulate a noncooperative game $\Gamma = \{\mathcal{P}, \mathcal{M}_{i\{i\in\mathcal{P}\}}, U_{i\{i\in\mathcal{P}\}}\}$ between N SUs and K eavesdroppers in the presence of M PUs. Our objective is to study and analyze the outcome from these interactions.

2.2 Game Solution

Here, we investigate the solution of the proposed finite noncooperative game Γ between SUs and eavesdroppers. In this chapter, we will use the term "player" to denote either an SU or an eavesdropper, unless an explicit distinction is needed.

2.2.1 Nash Equilibrium in Mixed Strategies and Fictitious Play

As a solution for the proposed game Γ, we use the concept of mixed-strategy Nash equilibrium defined as follows:

Definition 2.1. *A mixed strategy profile $\boldsymbol{p}^* = (\boldsymbol{p}_i^*, \boldsymbol{p}_{-i}^*)$ is said to be a* mixed strategy Nash equilibrium (MSNE) *if and only if it satisfies the following set of inequalities*

$$\bar{U}_i(\boldsymbol{p}_i^*, \boldsymbol{p}_{-i}^*) \geq \bar{U}_i(\boldsymbol{p}_i, \boldsymbol{p}_{-i}^*)\ \forall \boldsymbol{p}_i \in \Lambda_i\ \forall i \in \mathcal{P}. \tag{2.9}$$

The above definition implies that, whenever an MSNE is attained, no player has the incentive to unilaterally deviate and change its probability of channel selection. In other words, none of the SUs is capable of generating a

higher secrecy rate by unilaterally altering its current probability distribution over the channels. Similarly, none of the eavesdroppers is capable of further decreasing the secrecy rate of SUs through unilateral action. It is well known that, for a finite noncooperative game, a Nash equilibrium in mixed strategies always exists [37].

To reach an MSNE, an algorithm based on fictitious play (FP) can be used [38]. FP is a learning scheme in which players update their beliefs about their opponents by monitoring their actions. Since these actions are time dependent, we define $a_i(t)$ to be the channel chosen by player i at time t. Let $p_i^{a_i}(t),\ a_i \in \mathcal{M}_i, i \in \mathcal{P}$, be the empirical frequency, defined as the frequency with which player i has chosen action a_i until time t. For any time t, the following recurrence holds:

$$p_i^{a_i}(t) = \frac{t-1}{t} \cdot p_i^{a_i}(t-1) + \frac{1}{t} \cdot \mathbb{1}_{\{a_i(t-1)=a_i\}}. \tag{2.10}$$

FP proceeds as follows: at time t, player i observes the actions of all other players at time $t-1$, and then updates its knowledge of the frequencies. Using (2.10), player i computes $p_j^{a_j}(t)\ \forall a_j \in \mathcal{M}_j\,, \forall j \in \mathcal{P} \setminus \{i\}$.

In FP, the channels chosen at time t are the ones that maximize the expected utility with respect to the updated empirical frequencies. To reach an MSNE, players' strategies need to converge to p_i^*, the mixed strategy equilibrium that maximizes the expected value of the utility $\bar{U}_i(p_i, p_{-i}^*)$ as expressed in (2.8). To do so, player i's action at each time step maximizes the expected utility $\bar{U}_i(a_i, \boldsymbol{p_{-i}}(t))$ over the set of actions:

$$a_i(t) = \arg\max_{a_i \in \mathcal{M}_i} \bar{U}_i(a_i, \boldsymbol{p}_{-i}(t)). \tag{2.11}$$

$\bar{U}_i(a_i, \boldsymbol{p_{-i}}(t))$ represents the expected utility at the current time t, and it is given by:

$$\bar{U}_i(a_i, \boldsymbol{p}_{-i}(t)) = \sum_{\boldsymbol{a}_{-i} \in \mathcal{M}_{-i}} U_i(a_i, \boldsymbol{a}_{-i}) \prod_{a_j \in \boldsymbol{a}_{-i}} p_j^{a_j}(t), \tag{2.12}$$

where $\boldsymbol{p}_{-i}(t)$ represents the vector of empirical frequencies pertaining to the actions selected by all other players in $\mathcal{P} \setminus \{i\}$ as calculated by player i at time t. $\mathcal{M}_{-i} := \times_{j \in \mathcal{P} \setminus \{i\}} \mathcal{M}_j$ represents the space of all possible actions taken by all players other than i.

Based on their observations, the players first update their empirical fre-

quencies using (2.10), and then choose their actions as per (2.11).

As we have seen, the use of FP to find the MSNE of the proposed game requires each player to be able to observe the others' actions. For the eavesdroppers, there is a need to observe the channel selections of the SUs at time $t-1$. This can be done by monitoring the SUs' transmissions using known signal processing techniques [33].

The SUs need to be able to observe the channel choices of one another as well as the actions taken by the eavesdroppers. By monitoring the interference levels, either via measurements or through feedback from the base station [33], each SU can, at time t, observe the choices of other SUs at time $t-1$. In the proposed approach, the SUs do not need to observe the eavesdroppers' actions, which is often challenging in practice. Instead, by knowing or estimating the potential locations of eavesdroppers, the SUs can *predict the possible strategy choices* of the eavesdroppers. This is possible because, given the locations and the past actions, an SU is capable of deriving the best response of each eavesdropper. Note that the actions predicted are optimal for the eavesdroppers and accordingly the SUs are protecting themselves against the worst case scenario. In other words, if the eavesdroppers deviate from the predicted actions, the SUs will be better off.

2.2.2 Proposed Distributed Learning Algorithm

While FP can be used to find an MSNE, it often leads to extensive computational requirements especially when dealing with large cognitive networks. This can be clearly seen from (2.12) and (2.11). In order to overcome this issue, we propose a novel distributed learning algorithm that can reach an MSNE of the game at a much lower computational complexity relative to the standard FP.

Our proposed approach is inspired from regret matching techniques and the so-called Joint Strategy Fictitious Play (JSFP) introduced in [39]. The main idea is to enable the players to update their actions based on the regret for not choosing this action in the past. At time t, each player i has an expectation of its utility, $\bar{U}_i^{a_i}(t)$, if it chooses a_i. This expected utility has

the following update rule [39]:

$$\bar{U}_i^{a_i}(t) = \frac{t-1}{t} \cdot \bar{U}_i^{a_i}(t-1) + \frac{1}{t} \cdot U(a_i, \boldsymbol{a}_{-i}(t-1)), \tag{2.13}$$

where $\boldsymbol{a}_{-i}(t-1)$ represents the actions taken by all players other than i at time $t-1$ and $U(a_i, \boldsymbol{a}_{-i}(t-1))$ represents the utility of player i if it chose a_i at time $t-1$ and it can be computed using (2.7). By doing so, the players do not need to continuously calculate the expected utility as in (2.12), instead, they can update their expected utilities $\forall a_i \in \mathcal{M}_i$ as per (2.13).

Accordingly, the players update their actions at time t by maximizing their expectations of the utility over the action space:

$$a_i(t) = \arg \max_{a_i \in \mathcal{M}_i} \bar{U}_i^{a_i}(t). \tag{2.14}$$

Note that computing (2.11) has a worst-case complexity of $O\left(M^{N+K}\right)$ while computing (2.14) has a worst-case complexity of $O(M)$ only. Consequently, (2.13) and (2.14) can be readily computed even for large networks, unlike (2.11) and (2.12).

Based on this idea, we propose a Secure Channel Selection Algorithm (SCSA). SCSA is a low-complexity distributed learning algorithm that can be used by SUs and eavesdroppers to reach an equilibrium and it is divided into three main stages. In the first stage, both SUs and eavesdroppers choose the channels with equal probabilities as they do not have any observations on the state of the network initially.

The second stage is called fast learning. In this stage, the players learn about each others' decisions and choose their actions according to the update equations (2.13) and (2.14). Unlike classical regret matching such as in [39], our proposed approach allows the players to learn an MSNE, not a pure strategy NE. Therefore, the players will keep observing and updating the frequencies as per (2.10).

When the difference between all the calculated frequencies in consecutive time instants is within a certain threshold τ, the players switch to the third and final stage of the algorithm. In this stage, the players use the standard fictitious play process starting from the beliefs obtained in stage 2 until they converge to an MSNE. This algorithm is summarized in Algorithm 2.1.

In the proposed algorithm, the players will only switch to stage 3 after

Algorithm 2.1 Proposed Secure Channel Selection Algorithm

procedure SCSA STAGE 1 ▷ Initialization
    Each player $i \in \mathcal{P}$ chooses a random action $a_i(0) \in \mathcal{M}_i$.
end procedure

procedure SCSA STAGE 2 ▷ Fast Learning
    repeat
    Each player $i \in \mathcal{P}$ observes the actions of other players $\boldsymbol{a}_{-i}(t-1)$ and updates its average utility as per (2.13).
    Each player $i \in \mathcal{P}$ takes action $a_i(t)$ as per (2.14).
    Each player $i \in \mathcal{P}$ updates his knowledge of empirical frequencies $\boldsymbol{p}_{-i}(t)$ as per (2.10).
    until frequencies are within τ.
end procedure

procedure SCSA STAGE 3 ▷ Fictitious Play
    As a starting point for FP, players use the probabilities obtained in SCSA Stage 2.
    repeat
    Each player $i \in \mathcal{P}$ observes the actions of other players $\boldsymbol{a}_{-i}(t-1)$ and updates its knowledge of empirical frequencies $\boldsymbol{p}_{-i}(t)$ as per (2.10).
    Each player $i \in \mathcal{P}$ takes action $a_i(t)$ as per (2.11).
    until convergence to a MSNE.
end procedure

all frequencies are within the same τ, and therefore they are all guaranteed to start using standard fictitious play at the same instant. The idea behind SCSA is to reduce the number of iterations required by FP by allowing the players to pursue a network learning phase prior to engaging into equilibrium learning through FP. This renders the problem of finding an MSNE for the game less complex. Given that the last stage of the proposed algorithm is based on FP, when it converges, we are guaranteed to reach an MSNE of the game. We note that, in general, fictitious play does not converge for all types of games; however, many modification schemes have been suggested to ensure its convergence [38].

Remark 2.1. *The game considered in this chapter may have multiple MSNEs and our proposed algorithm converges to only one of these, which naturally depends on the starting point. Our particular selection is a very general network state, where players have no knowledge of the network and start by choosing random actions. We note that the proposed algorithm can also accommodate*

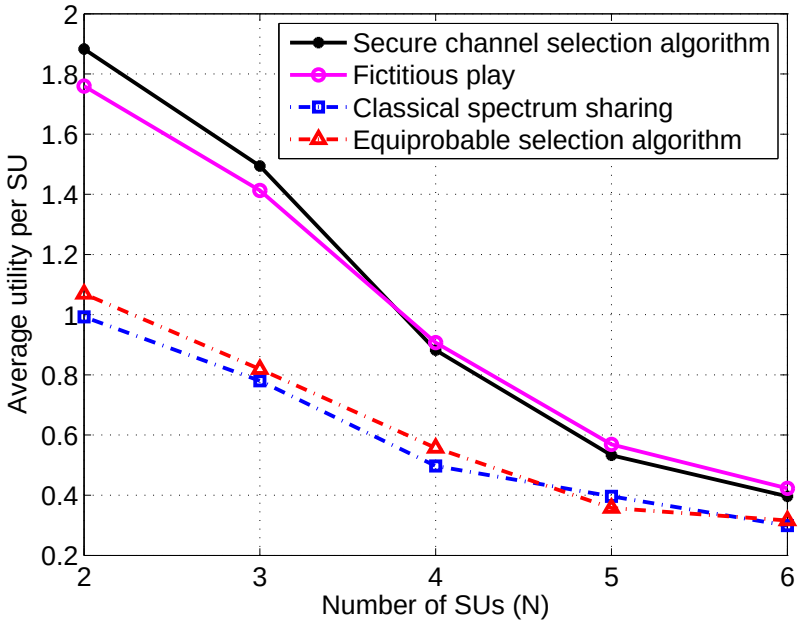

Figure 2.2: Average utility per SU resulting from SCSA, FP, equiprobable selection, and classical spectrum sharing as the number N of SUs varies for $K = 3$ eavesdroppers.

other starting network states as well. Moreover, advanced spectrum sharing techniques can also be incorporated [20].

2.3 Simulations and Results

For simulations, we set up the following network: the BS is located at the center of a 750 m×750 m square with the SUs and eavesdroppers randomly placed in this area. The secondary users' transmit power level $P_{i,m}$ is set to 10 mW $\forall m \in \mathcal{M}_i\,, \forall i \in \mathcal{N}$. Unless otherwise specified, we consider a network of $M = 3$ channels. The number of SUs and eavesdroppers are different for each simulation scenario and they will be specified. We set the noise level to $\sigma^2 = -90$ dBm, the path loss exponent to $\mu = 3$ and the path loss constant is to 1. For SCSA, we set the threshold after which players switch to FP to $\tau = 10^{-2}$. All the obtained results are averaged over random positions of SUs and eavesdroppers, channel gains, and channel availability θ_m.

To evaluate the performance of the proposed SCSA algorithm, we show, in Figure 2.2, the average expected utility achieved by the SUs as the number

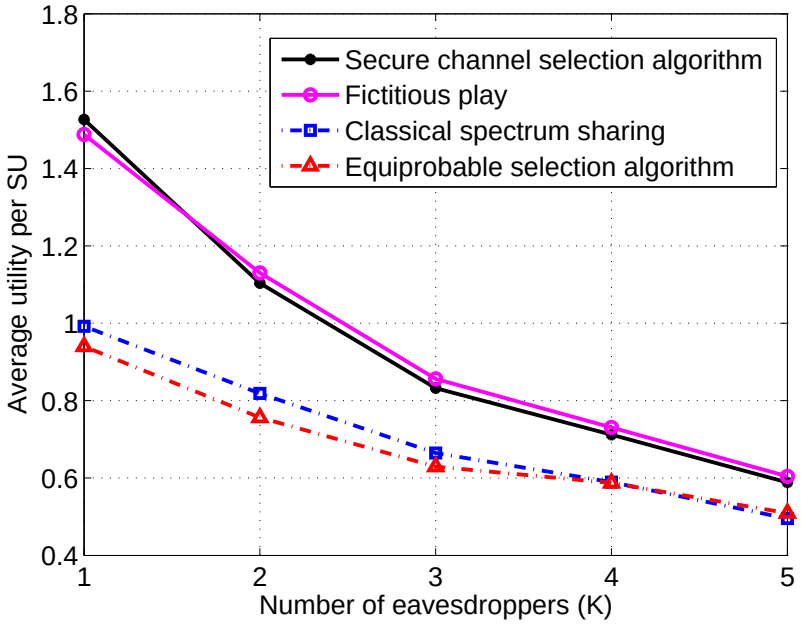

Figure 2.3: Average utility per SU resulting from SCSA, FP, equiprobable selection, and classical spectrum sharing as the number K of eavesdroppers varies for $N = 4$ SUs.

N of SUs increases for a network with $K = 3$ eavesdroppers. The performance of our approach is compared to that of a classical spectrum sharing algorithm, in which SUs keep optimizing their capacities given by (2.2) until all channel selections converge. Also, SCSA is compared to standard FP and to an equiprobable channel selection algorithm, in which all SUs choose channels with equal probabilities. Figure 2.2 shows that as the number N of SUs increases, the average utility per SU decreases for all four schemes. This is due to the fact that the SUs are utilizing the channels more, and hence the mutual interference between them is increasing. We can clearly see from Figure 2.2 that the proposed algorithm and FP have comparable performances while they both outperform the other two approaches. Figure 2.2 shows that the proposed SCSA scheme yields a significant improvement, in terms of the average utility per SU, at all N. This improvement varies between 76.2% and 89.7% at $N = 2$ to 25.4% and 32.7% at $N = 6$, relative to equiprobable selection and classical spectrum sharing, respectively. Due to the presence of multiple MSNEs, FP and SCSA may converge to different equilibrium points with different average utilities. Consequently, in such a scenario, SCSA can possibly outperform FP on the average and vice versa.

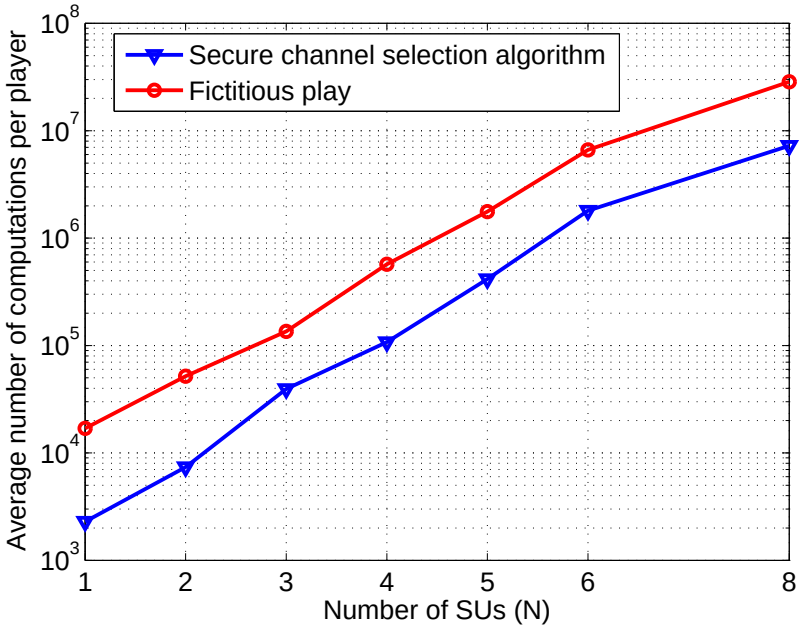

Figure 2.4: Average number of computations per player resulting from both SCSA and FP as the number of SUs, N, varies for $K = 3$ eavesdroppers.

Figure 2.3 shows the average expected utility achieved by the SUs as the number K of eavesdroppers increases for a network with $N = 4$ SUs. We notice that as the number of eavesdroppers increases, the average utility per SU decreases for all four schemes. This is a result of the fact that an increase in the number of eavesdroppers will further decrease the overall secrecy rate of the SUs. In Figure 2.3, we can see that SCSA and FP have a comparable performance while they both outperform the other two approaches. In this respect, Figure 2.3 shows that the proposed SCSA scheme yields a significant improvement, in terms of the average utility per SU, at all K. This improvement varies between 62.4% and 53.9% at $K = 1$ to 15.6% and 18.8% at $K = 5$, relative to equiprobable selection and classical spectrum sharing, respectively.

In Figure 2.4 we show the computational performance of our proposed secure channel selection algorithm versus FP as the number of SUs, N, increases in the network. We assess the computational needs of both learning schemes in terms of the average number of utility computations, as per (2.7), performed per player in order to converge to an MSNE of the game. Figure 2.4 shows that, as the number N of SUs in the network increases, the average number of utility computations done by each player increases expo-

nentially in both algorithms. This is due to the fact that, as N increases, each SU i will have to consider a larger set of action space $\mathcal{M}_{-i}$ when calculating its expected utility. We note that the exponential increase in FP is due to the fact that computing (2.11) has a worst-case complexity of $O\left(M^{N+K}\right)$. The increase in complexity of the proposed secure channel selection algorithm is due to the use of FP at stage 3. Figure 2.4 shows that the proposed SCSA achieves significant reductions in terms of computation as it requires 86.5% and 74.6% less computation than fictitious play at $N = 1$ and $N = 8$, respectively.

CHAPTER 3

CR NETWORK SECURITY: PARTIAL KNOWLEDGE

In this chapter, we discuss the ability of the SUs to evade eavesdroppers in CR networks while maintaining quality-of-service guarantees for the PUs. Here, we assume that the SUs have only partial knowledge about the locations of eavesdroppers. In addition, we consider an advanced eavesdropping model, different than the one discussed in Chapter 2. In this model, a continuum of eavesdroppers that can simultaneously wiretap all channels is present.

The objective of the SUs is to ensure a secure link with the BS without incurring high interference levels on the PU channels at all times. To address this problem, we consider the case in which the SUs are mobile and are able to change their locations in the network. This can be the case of military vehicles moving in the battlefield, mobile users moving using their cars on highways, or even pedestrians walking around in cities. For example, as eavesdropping attacks are common in military scenarios, accommodating for their presence is a must when moving military vehicles around. Moreover, the government can identify the names of streets and areas that are high-risk and are known for previous eavesdropping activities and provide this information to the SUs and the BSs. This would aid in finding safer routes for commuting SUs. So, the secondary users will mitigate the effect of the eavesdroppers by changing their locations.

The chapter is organized as follows: in Section 3.1, we introduce the system model and formulate the utility of the SUs. In Section 3.2, we provide the proposed solution approaches and in Section 3.3, we analyze the simulation results.

3.1 System Model and Utility Formulation

3.1.1 System Model

Consider a cognitive radio network comprised of a set $\mathcal{M}$ of M licensed primary users (PUs) or channels which can be accessed by a set $\mathcal{N}$ of N unlicensed secondary users (SUs). The objective of each SU is to securely communicate with a common base station (BS) by using one of the PU channels in the presence of eavesdroppers. Eavesdroppers are passive devices that can decode the user messages on all channels, thus threatening the confidentiality of the transmitted information. They are spread over a set $\mathcal{K}$ of K circular areas. The centers and radii of these areas, and not the exact locations of eavesdroppers, are known to the SUs, PUs, and the BS. In each circular area k, eavesdroppers are assumed to be uniformly distributed with density λ_k eavesdroppers per unit area.

In such a cognitive network, the SUs must maintain a certain interference level at each channel so that the PUs can achieve their quality-of-service guarantees. This is captured by keeping the actual interference on channel m below the threshold level $\tilde{I}_m$ at all times. Moreover, SUs must not interfere with the PUs' signal reception. To this end, we assign to each PU a footprint that represents an area free of SU transmissions [40]. We denote by $\mathcal{X}_m$ the footprint area of PU m. Inside $\mathcal{X}_m$, only the PU m is allowed to transmit its signal on channel m guaranteeing the PU a low interference medium around its RF receiver. For the channel, we assume a different model than the one in Chapter 2. Here, the signal attenuates with the distance d according to $\kappa d^{-\mu}$, where κ is the path loss constant and μ is the path loss exponent.

To model the movement of the SUs, we partition the network over which the SUs are spread into $v \times v$ congruent square areas. At each time step, each SU must be at one of the $(v+1)^2$ vertices. Without loss of generality, for tractability, we assume that each SU is allowed to move only once to one of the neighboring vertices, at each time instant. Therefore, at each time step, an SU has to choose one of the following actions:

1. Send directly on one of the available channels.

2. Send at the next time step from the current location on one of the available channels.

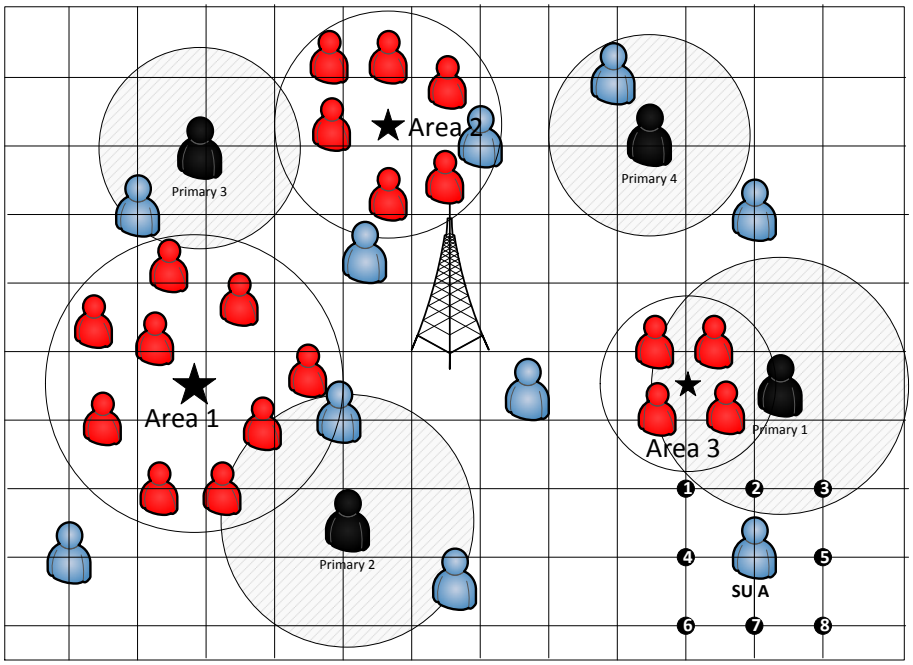

Figure 3.1: Illustrative example of the proposed system model.

3. Move to one of the neighboring locations and then send on the next time step on one of the available channels.

Accordingly, SU i's action is represented by the triplet (τ, j, m), with τ the number of time steps SU i waits before transmission, j the location from which SU i sends its data, and m the chosen channel. Figure 3.1 shows an illustrative example of a CR network with 10 SUs, 4 PUs, and a number of eavesdroppers spread over 3 areas. Note that the number of available channels is not necessarily M on all positions in the network as an SU present inside a PU's footprint is unable to send on its channel. For example, SU A shown in Figure 3.1 is unable to send on channel 1 from positions 2 and 3 as they happen to be inside $\mathcal{X}_1$, PU 1's footprint area.

3.1.2 Utility Formulation

In general, each SU i will choose the action that will maximize its utility function U_i. This function captures the SU's probability of secure communication, time delay, movement costs, and PU footprint. First, we discuss the effect of each one of these aspects on the SU and then summarize these

findings to formalize the utility function.

Secrecy

Physical layer (PHY) security techniques, introduced in [9], are extensively used to address eavesdropping related problems. It has been shown, by an information theoretic analysis, that under certain conditions, an SU is able to send its data securely in the presence of eavesdroppers. These conditions can be summarized by the following: the channel between this SU and the BS has to have a higher gain than that between the SU and the most damaging eavesdropper [9]. Under the path loss channel model considered in this chapter, the channel has a higher gain as the separating distance becomes smaller. In other words, if the BS is closer to the SU than any other eavesdropper, the SU's data can be sent securely.

In each area k, eavesdroppers are uniformly and independently distributed with a constant density λ_k. Using stochastic geometry, eavesdroppers' locations can be modeled as a stationary Poisson point process with density λ_k [41]. Under this model, the probability that no eavesdropper is present inside a given region $\mathcal{A}$ is given by $e^{-\lambda_k A}$, with A the area of $\mathcal{A}$ [41].

Therefore, the probability that an SU i can send its data securely, is given by:

$$p_i = \prod_{k=1}^{k=K} e^{-\lambda_k A_k}. \tag{3.1}$$

Here, A_k represents the area of the region defined by the intersection of the following two circles: the first is the circle of eavesdroppers k, and the second is the circle centered at the SU i with radius d, the distance from SU i to the BS.

Remark 3.1. *Note that $A_k = 0$ for all k and p_i evaluates to 1 when the BS is closer to SU i than any other eavesdropper. Also, the probability of secure transmission is independent of the channel choice since all channels are facing the same eavesdropping attack.*

An illustrative example is shown in Figure 3.2. Here, the BS is closer to SU 1 than any other eavesdropper and hence SU 1 can send its data securely with probability 1. In contrast, SU 2 can send its data securely only if no

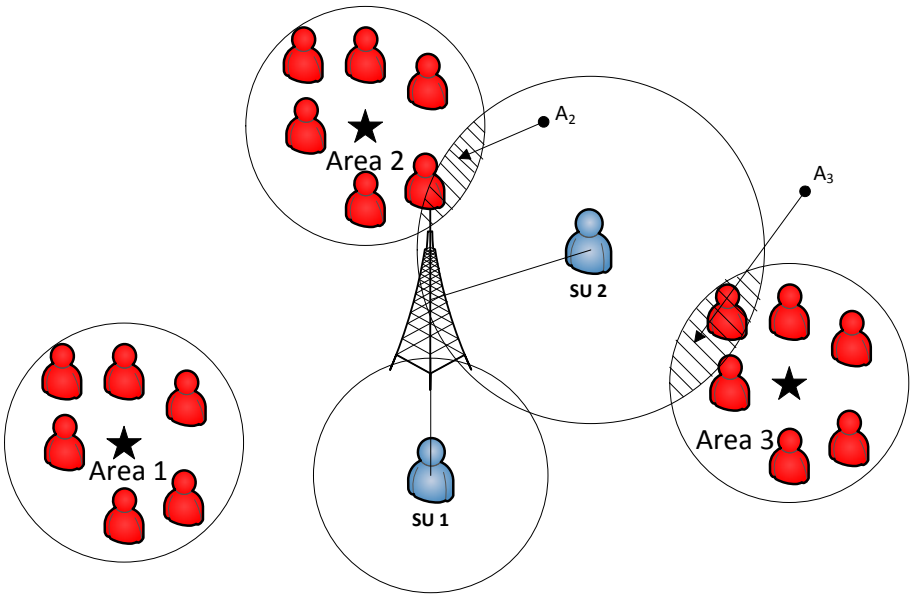

Figure 3.2: Illustrative example of eavesdropping.

eavesdropper is present in both $\mathcal{A}_2$ and $\mathcal{A}_3$. Therefore, p_2, the probability that SU 2 can send its data securely is given by:

$$\begin{aligned} p_2 &= \prod_{k=1}^{k=3} e^{-\lambda_k A_k} \\ &= e^{-\lambda_1 A_1} \times e^{-\lambda_2 A_2} \times e^{-\lambda_3 A_3} \\ &= e^{-\lambda_1 A_2} \times e^{-\lambda_2 A_3}, \end{aligned}$$

where A_2 and A_3 represent the areas of the shaded regions $\mathcal{A}_2$ and $\mathcal{A}_3$ in Figure 3.2. A_1 is zero since circle around the SU 1 does not intersect with the eavesdropping area 1.

Time delay

In addition to secure communication, the SUs are interested in sending their time sensitive data to the BS promptly. So, each message is assigned a time-out, τ_{max}, representing the maximum allowed delay for this message. Accordingly, when an SU delays its data transmission, its utility decreases, until it diminishes when the delay becomes larger than or equal to τ_{max}. We capture this by adding an exponential decay to the utility function: $\exp\left(\frac{-\tau}{\tau_{max}-\tau}\right)$,

where τ represents the delay that the message experiences before being sent. For example, if an SU has a utility $U(0)$ at $t = 0$, after τ time steps the utility will be $U(\tau) = \exp\left(\frac{-\tau}{\tau_{max}-\tau}\right) \times U(0)$.

Movement costs

An SU's mobility incurs a cost that is modeled by adding a constant scalar η for each time the SU changes its location to one of its neighboring vertices. The presence of this cost differentiates between the following two actions: the first is to wait and send on the next time step, while the second is to move and send on the next time step.

PU footprint

In order to minimize the interference with the PUs' receivers, the SUs must not send on channel m if it is inside PU m's footprint area. To enforce this, we say that the utility of an SU i sending on channel m from position j is zero when $j \in \mathcal{X}_m$.

Action Space

As previously discussed, an SU's action is represented by the triplet (τ, j, m). The number of available channels is M, and hence $m \in [1, M]$. Since the message's timeout is τ_{max}, then $\tau \in [0, \tau_{max} - 1]$. The number of available positions for an SU depends on its location and τ_{max}. In general, as an SU can only move once per time step, the maximum number of possible locations can be easily shown to be $(2\tau_{max} - 1)^2$. Hence, A_i, the action space of SU i, is:

$$A_i = [0, \tau_{max} - 1] \times [1, M] \times [1, (2\tau_{max} - 1)^2] \tag{3.2}$$

In this chapter, we define $a_i := (\tau, j, m)$ to represent the action of SU i, with $a_i \in A_i$.

Remark 3.2. *The number of available actions for each SU is the cardinality*

of A_i and it is given by:

$$|A_i| = \sum_{\tau=0}^{\tau_{max}-1} M \cdot (2\tau + 1)^2 = \frac{M}{3} \cdot \tau_{max} \cdot (4\tau_{max}^2 - 1). \tag{3.3}$$

In summary, we propose the following utility that captures all the aforementioned aspects for each SU i that chooses an action $a_i = (\tau, j, m)$:

$$U_i(a_i) := \begin{cases} -\tau_j \cdot \eta & \text{if } j \in \mathcal{X}_m \text{ or } \tau \geqslant \tau_{max}, \\ p_{i,j} \cdot \exp\left(\frac{-\tau}{\tau_{max}-\tau}\right) - \tau_j \cdot \eta & \text{else,} \end{cases} \tag{3.4}$$

where $p_{i,j}$ represents the probability that SU i can securely transmit its data at location j and it is given by (3.1). The term τ_j is the minimum number of steps the SU i needs to reach position j, and $\tau_j \in [0 \;\; \tau_{max} - 1]$. Note that τ_j is not necessarily the same as τ as the SU may decide to wait and send on the next time step without changing its location.

3.2 Proposed Solution

In the studied model, the objective is to choose the optimal actions for the SUs so as to maximize their social welfare, i.e. $\sum_{i \in \mathcal{N}} U_i(a_i)$. This optimization problem is subject to the constraints dictated by the PUs' interference thresholds set on each channel.

We present three different approaches to solve this optimization problem. In the first approach, we study the centralized solution, assuming that the BS has perfect knowledge of the SUs' locations and utilities. In the second, we study a decentralized game theoretic approach in which the SUs communicate at each time step. Finally, we introduce the decentralized Lagrangian heuristic approach in which the SUs can only communicate with the BS that has no information about the SUs' utilities.

3.2.1 Centralized Solution Approach

In this section, we formulate the optimization problem and present a centralized optimal solution approach to solve it. The centralized problem is solved by the BS that has access to the information about the SUs and their

utilities, the PUs and the areas where eavesdroppers are present. In this regard, the problem can be formulated as:

$$\begin{aligned} &\max_{\mathbf{a}\in\mathcal{A}_1\times\cdots\times\mathcal{A}_N} \sum_{i\in\mathcal{N}} U_i(a_i), \\ &\text{subject to } \; I_{m,\tau} \leqslant \tilde{I}_{m,\tau} \; \forall \tau < \tau_{max}\,, \forall m \in \mathcal{M} \end{aligned} \tag{3.5}$$

where $I_{m,\tau}$ represents the level of interference at the BS on channel m at time τ caused by the SU transmissions, $\tilde{I}_{m,\tau}$ is the maximum allowed interference as set by the PUs, and $\mathbf{a}$ is the vector $a_1, a_2, \ldots, a_N$ of the SU actions.

The BS's goal is to choose the action vector $\mathbf{a}$ that maximizes the social welfare of the SUs in the presence of PUs and eavesdroppers. In other words, the BS assigns for each SU the appropriate channel, sending location and transmission time.

To solve this problem, we first cast it as a binary integer program. Here, for each SU i, channel m, position j and time τ, we assign a binary variable $x_{i,\tau,j,m}$. Accordingly, the objective function to be maximized can be equivalently written as $\sum_{i,\tau,j,m} U_i(\tau, j, m) \cdot x_{i,\tau,j,m}$. This new formulation adds the following constraint: for each SU i, at most one of x_i's can be set to 1. This means that, if $x_{i,\tau,j,m} = 1$, then the action taken by SU i is $a_i = (\tau, j, m)$. We now formulate the binary integer program that is equivalent to the problem in (3.5):

$$\begin{aligned} \max f(x) &= \sum_{i,\tau,j,m} U_i(\tau, j, m) \cdot x_{i,\tau,j,m} \\ \text{subject to} &\sum_{\tau,j,m} x_{i,\tau,j,m} \leqslant 1, \qquad \forall i \in \mathcal{N}. \\ &\sum_{i} x_{i,\tau,j,m} \cdot I\,(i,j) \leqslant \tilde{I}_{\tau,m}, \forall \tau < \tau_{max}\,, \forall m \in \mathcal{M}, \\ &x_{i,\tau,j,m} \in \{0,1\}. \end{aligned} \tag{3.6}$$

$I(i,j)$ represents the interference at the BS when SU i sends its data from location j and it is given by:

$$I(i,j) = P_i d_j^{-\mu},$$

with P_i the power of the signal transmitted by SU i and d_j the distance

between location j and the BS.

Notice that the problem formulated in (3.6) is actually a General assignment problem (GAP). This problem has been extensively studied in the literature and there are many efficient algorithms to solve it [42]. The solution to the proposed GAP in (3.6) is the optimal solution for the centralized problem discussed in (3.5) since both problems are equivalent.

3.2.2 Decentralized Game Theoretic Approach

In this section, we consider the case in which each SU maximizes its own utility U_i, instead of maximizing the social welfare. Although the utility U_i is a function of a_i only, the set of admissible actions for SU i is determined by $\mathbf{a}_{-i} := \{a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_N\}$, the actions of all the SUs other than i. In this case, we say that the constraints are *interdependent* and the actions of the SUs are coupled. This coupling stems from the constraints and this renders the problem game theoretic [43]. We note that this game is not a classical noncooperative game. In classical noncooperative game theory, the utility of a player is a function of the actions taken by (a subset of) all players [37]. In this scenario, we assume that each SU is able to communicate with the BS and all the other SUs. We now formulate a decentralized game theoretic version of the problem in (3.5).

Now, each SU i solves the following optimization problem:

$$\begin{aligned} \max_{a_i \in \mathcal{A}_i} \quad & U_i(a_i) \\ \text{subject to} \quad & I_{m,\tau} \leqslant \tilde{I}_{m,\tau}, \ \forall \tau < \tau_{max} \ , \forall m \in \mathcal{M}. \end{aligned} \tag{3.7}$$

Denote by $\tilde{\mathcal{A}}_i(\mathbf{a}_{-i})$ the action set $\mathcal{A}_i$ subject to the constraints in (3.7) as determined by the actions $\mathbf{a}_{-i}$, so that SU i's problem becomes:

$$\max_{a_i \in \tilde{\mathcal{A}}_i(\mathbf{a}_{-i})} \quad U_i(a_i) \tag{3.8}$$

Therefore, the problem described in (3.8) is a generalized game with coupled constraints [43] whose solution is the Generalized nash equilibrium (GNE). The GNE is more general than the ordinary Nash equilibrium as it accounts for the coupling in the action sets too, and it is defined below.

Definition 3.1. *A GNE is the vector* $\bar{\mathbf{a}}$ *such that for all* $i \in \mathcal{N}$, $a_i = \arg\max_{a_i \in \tilde{\mathcal{A}}_i} U_i(a_i)$ *with* $\tilde{\mathcal{A}}_i = \tilde{\mathcal{A}}_i(a_{-i})$.

After examining the game formulation, we can state the following proposition.

Proposition 3.1. *The game presented above is a generalized potential Nash game.*

Proof. Consider the function $f(x) = \sum_i f_i(x)$. This function is a potential function of the game since each $f_i(x)$ depends on x_i only. The generalized potential function is given in Definition 2.1 in [43]. □

To solve this problem and find the GNE of the game, we first transform it into a binary integer program similar to the one in (3.6). So, for each SU i the problem is equivalent to:

$$\begin{aligned} \max f_i(x) &= \sum_{\tau,j,m} U_i(\tau, j, m) \cdot x_{i,\tau,j,m} \\ \text{subject to} \sum_{\tau,j,m} x_{i,\tau,j,m} &= 1, \\ \sum_{i,j} x_{i,\tau,j,m} \cdot I\,(i,j) &\leqslant \tilde{I}_{\tau,m}, \forall \tau < \tau_{max}\ , \forall m \in \mathcal{M}, \\ x_{i,\tau,j,m} &\in \{0,1\}. \end{aligned} \tag{3.9}$$

We now propose the following algorithm, called the Iterative Constrained Best Response (ICBR) algorithm. Initially, $\tilde{I}$ is initialized to the requirements set by the PUs. Then, randomly and sequentially, each SU chooses the action that maximizes its utility according to the available channel constraints. In other words, the user solves the optimization problem in (3.9). When an SU chooses to send at time τ and channel m from position j, the corresponding $\tilde{I}_{\tau,m}$ will be updated to $\tilde{I}_{\tau,m} = \tilde{I}_{\tau,m} - I_j$ and broadcast to all the SUs. The other SUs will now solve the problem (3.9) with the updated $\tilde{I}$. Finally, after the first round is over, each SU solves (3.9) again for the optimal solution with the available constraints. This is repeated until convergence. This algorithm is summarized in Algorithm 3.1.

Algorithm 3.1 Iterative Constrained Best Response (ICBR)

procedure ICBR STAGE 1 ▷ Initialization
    $\tilde{I}_{m,\tau}$ is initialized to the original interference constraint as given by the PUs.
end procedure

procedure ICBR STAGE 2 ▷ Optimization
    repeat
    Each SU i solves the optimization problem in (3.9) with the available constraints $\tilde{I}_{m,\tau}$. The action (j, τ, m) obtained is the best response.
    According to the chosen action (j, τ, m), $\tilde{I}_{m,\tau}$ is updated to $\tilde{I}_{m,\tau} - I(j)$.
    until actions converge.
end procedure

Remark 3.3. *The ICBR algorithm is actually a nonlinear Gauss-Seidel best response algorithm. It is guaranteed to converge for generalized potential Nash games with coupled action sets and objective functions that are independent from the actions of other users [43, 44].*

3.2.3 Distributed Lagrangian Approach

In this section we present a distributed optimization approach for solving the problem in (3.5). The approach discussed here is a Lagrangian relaxation of the GAP in (3.6). Note that, in this scenario, we assume that the BS has no information about the SUs and their utilities. Also, the SUs have minimal communication capabilities and they can only communicate with the BS.

Define the Lagrangian $L(x, \lambda)$ by incorporating the coupled constraints $\sum_i \sum_j x_{i,\tau,j,m} \cdot I_{i,\tau,j,m} \leqslant \tilde{I}_{\tau,m}$ into the objective function:

$$\begin{aligned} L(x,\lambda) = & \sum_{i,\tau,j,m} -U_i(\tau,j,m) \cdot x_{i,\tau,j,m} \\ & + \sum_{m,\tau} \lambda_{\tau,m} \cdot \left(\sum_{i,j} x_{i,\tau,j,m} \cdot I_{i,\tau,j,m} - \tilde{I}_{\tau,m} \right) \\ = & \sum_{i} \sum_{\tau,j,m} \left(-U_i(\tau,j,m) + \lambda_{\tau,m} \cdot I_{i,\tau,j,m}\right) \cdot x_{i,\tau,j,m} \\ & - \sum_{m,\tau} \lambda_{\tau,m} \cdot \tilde{I}_{\tau,m}. \end{aligned} \tag{3.10}$$

Algorithm 3.2 Distributed Lagrangian Optimization (DLO)

procedure DLO STAGE 1 ▷ Initialization
    $\hat{\lambda}^{(0)}$ is initialized to zeros. Set $t = 0$ initially.
end procedure

procedure DLO STAGE 2 ▷ Optimization
    repeat
    Each SU i solves the optimization problem in (3.12) to find $\hat{x}_i^t$ for $\lambda = \hat{\lambda}^{(t)}$. $\hat{x}_i^t$ and the corresponding $I(i,j)$ are transmitted to the BS.
    The BS broadcasts the new values of $\hat{\lambda}^{(t+1)}$ as per (3.14).
    until actions converge.
end procedure

And now, we minimize the Lagrangian to find $d(\lambda)$:

$$d(\lambda) = \min_{x} L(x, \lambda). \tag{3.11}$$

We can see that the objective function in (3.10) is separable, and accordingly the problem that each SU i solves is finding $\hat{x}_{i,\tau,j,m}$ for a fixed i and for all (τ, j, m) that solves:

$$\begin{aligned} \min_{x} & \sum_{\tau,j,m} \left(-U_i(\tau,j,m) + \lambda_{\tau,m} \cdot I_{i,\tau,j,m}\right) \cdot x_{i,\tau,j,m} \\ \text{subject to} & \sum_{\tau,j,m} x_{i,\tau,j,m} = 1 \\ & x_{i,\tau,j,m} \in \{0,1\}. \end{aligned} \tag{3.12}$$

Solving (3.12) becomes very simple as the SU i sets $\hat{x}_{i,\tau,j,m}$ to one and all other $\hat{x}_i$'s to zero when (τ, j, m) minimizes $(-U_i(\tau,j,m) + \lambda_{\tau,m} \cdot I_{i,\tau,j,m})$. The solution of (3.12) becomes optimal when λ is equal to λ^* which is the solution of:

$$\lambda^* = \arg\max_{\lambda \succcurlyeq 0} d(\lambda). \tag{3.13}$$

Obtaining the optimal value for λ^* is a very difficult and challenging problem in GAP relaxations [45,46]. Accordingly, we present here a heuristic suboptimal approach, which we call the Distributed Lagrangian Optimization (DLO) algorithm, to arrive at the vector $\hat{\lambda}$ that allows the SUs to choose their actions distributively without violating the coupled constraints. In order to

find $\hat{\lambda}$ and $\hat{x}$, we present an algorithm based on the well-known subgradient method [47]. First at time $t = 0$, the vector $\hat{\lambda}^{(0)}$ is initialized to zeros, and then each SU solves the optimization problem in (3.12). The results, $\hat{x}^t$ and the corresponding interference $I(i,j)$, are sent to the BS which in turn checks if the solution obtained is feasible by verifying the conditions: $\sum_i \sum_j \hat{x}^t_{i,\tau,j,m} \cdot I(j) \leqslant \tilde{I}_{\tau,m}, \forall\tau \ \forall m$. If one or more are violated, the BS updates the value of λ using the update rule:

$$\hat{\lambda}^{(t+1)}_{\tau,m} = \left(\hat{\lambda}^{(t)}_{\tau,m} + l(t) \times \left(\sum_{i,j} \hat{x}^t_{i,\tau,j,m} \cdot I(i,j) - \tilde{I}_{\tau,m} \right) \right)^+, \tag{3.14}$$

where $l(t)$ is the step size with $l(0) = 1$ and it is updated by $l(t+1) = l(t)/2$ every h iterations. Now, the BS sends the updated vector λ^{t+1} to the SUs which in turn solve the problem in (3.12) again. When (3.14) converges, i.e. $\hat{x}$ obtained from SUs is feasible and no need for an update, we stop iterating. The DLO algorithm is summarized here in Algorithm 3.2.

Note that there are many other algorithms that can lead to a better approximation of the optimal value x^*, but they require additional computational complexity and complete knowledge of the network and SU utilities at the BS [46]. The above algorithm is simple and does not require the BS to have any information about the network or the SUs.

3.3 Simulations and Results

For simulations, we consider a 500 m×500 m square area with the BS at the center. The number of SUs N and the number of areas with eavesdroppers K are varied within this area. Unless otherwise specified, we set the number of squares to $v = 20$, the number of channels to $M = 2$, the eavesdropper area radius to 30 m, and the PU footprint radius to 10 m. The SU transmit power is set to $P = 100$ mW. The wireless medium has a path loss exponent $\mu = 3$, a path loss constant $\kappa = 1$ and a noise level $\sigma^2 = -90$ dBm. We set the movement cost to $\eta = 0.01$. All statistical results are averaged over multiple random runs for different positions of eavesdroppers PUs and SUs.

In Figure 3.3, we show the average utility per SU as the number of SUs, N, increases in the network for $\tilde{I} = 3 \times 10^{-9}$ and $\tau_{max} = 2$. The results show

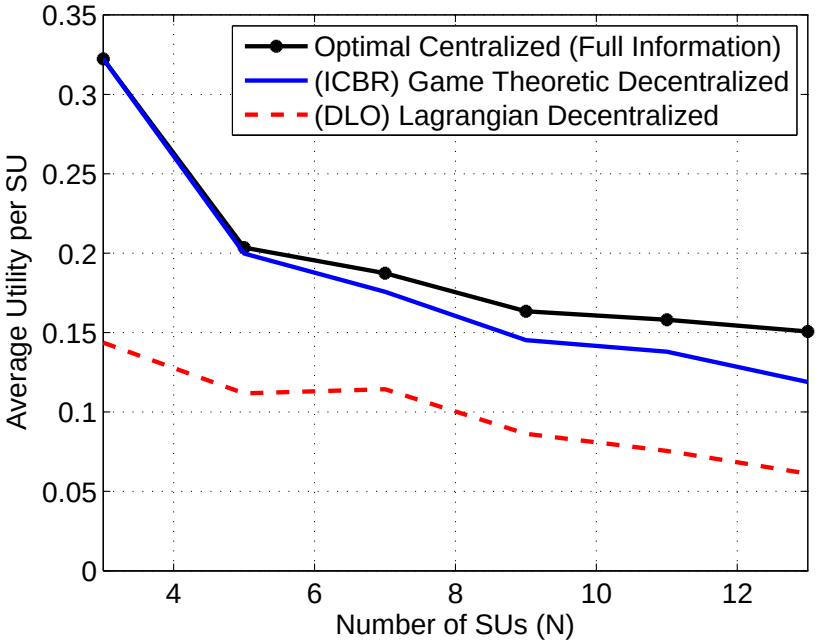

Figure 3.3: The average utility per SU as the number of SUs N increases.

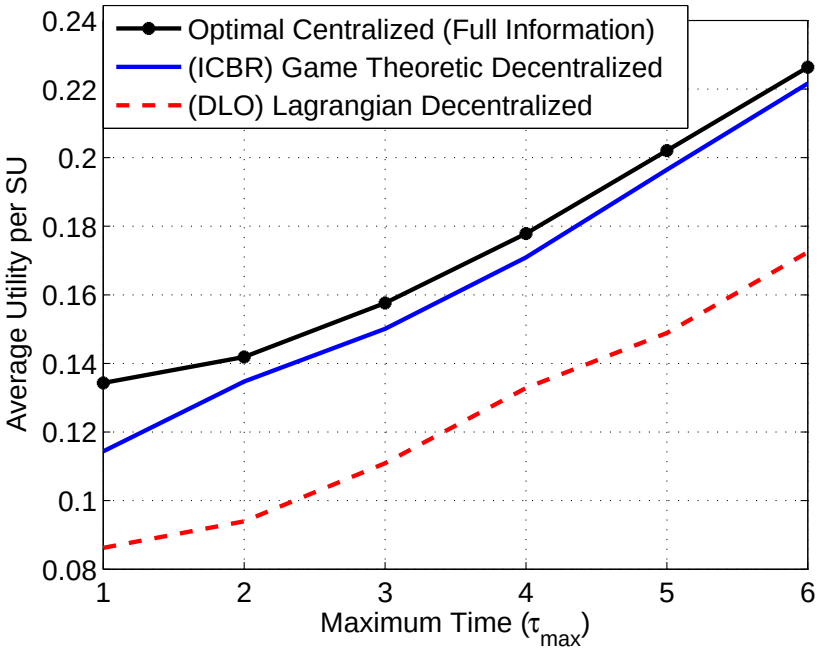

Figure 3.4: The average utility per SU as τ_{max} increases.

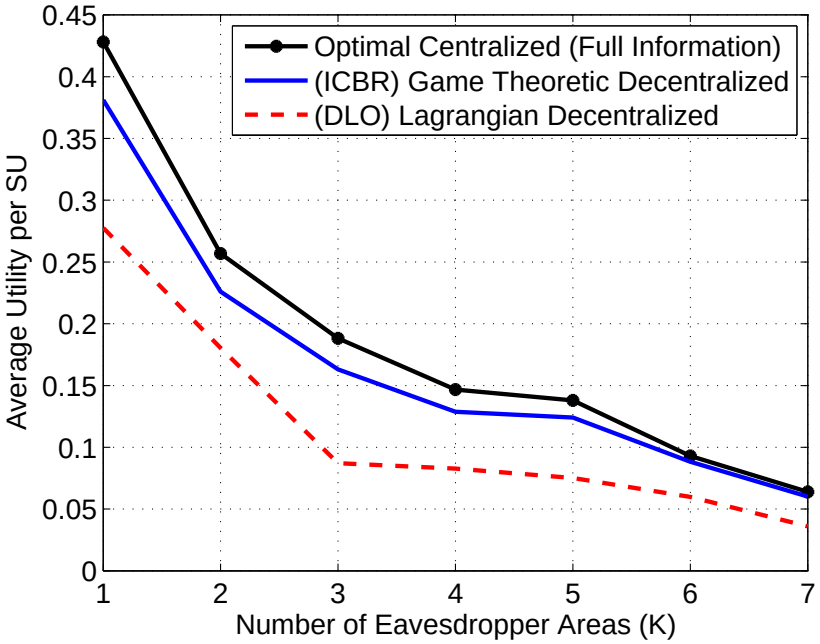

Figure 3.5: The average utility per SU as the number of areas with eavesdroppers K increases.

that as N increases, the average utility per SU decreases slowly. Indeed, we can see that the SUs' performance was degraded by 50% on average when N was increased by a factor of 4 (from $N = 3$ to $N = 12$). This result is due to the fact that, with the available time, interference threshold, and channels, the network can accommodate more SUs. As expected, Figure 3.3 clearly shows that the optimal algorithm with full information outperforms the non-optimal ones. The ICBR algorithm was near-optimal and only 11% less than the optimal value in the worst case with much less information. The DLO algorithm was able to perform well without the SUs communicating and it was 60% to 40% less than the optimal performance. We notice that the ICBR algorithm was able to benefit from the communication links between the SUs, a property that the DLO algorithm lacks.

In Figure 3.4, we show how the increase in the message timeout, τ_{max}, affects the average utility per SU. In this figure, we can see that, as the message timeout increases, the average utility per SU increases. This is due to the fact that as τ_{max} increases, the SUs will have more time to transmit and thus they are able to move and reach a larger subset of the network. The

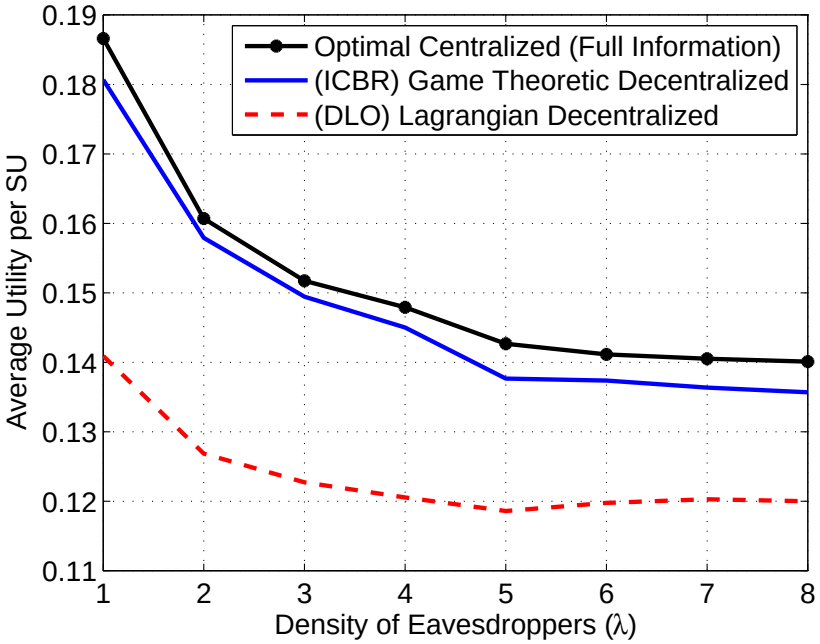

Figure 3.6: The average utility per SU as the density of eavesdroppers λ increases.

optimal centralized algorithm with full information clearly outperformed the decentralized ICBR and DLO algorithms. Here, the ICBR algorithm was 15% and 2% less than the optimal value at $\tau_{max} = 1$ and $\tau_{max} = 6$, respectively. For these same values of τ_{max}, the DLO algorithm was 35% and 24% less than the optimal value, respectively. Here, we can also see that, as the resources become more abundant, the price of SU selfishness decreases. Again, the ICBR outperformed the DLO algorithm as the communication between SUs helped in increasing the overall social welfare.

Figure 3.5 shows how increasing the number of areas with eavesdroppers, K, affects the average overall utility per an SU. In general, as the number of areas, K, increases, the average utility per SU decreases for all algorithms. This is due to the fact that with more eavesdroppers, the probability of secure transmission decreases. Also, SUs will have to move longer distances to evade potential eavesdropping, thus incurring movement costs and delays. The optimal algorithm outperformed the decentralized ones. Here, both the ICBR and DLO algorithms achieved near-optimal results. In the worst case, the ICBR and DLO algorithms were 11% and 29% less than the optimal

value, respectively.

We show in Figure 3.6 the average utility per SU as λ, the density of eavesdroppers, increases. We notice that, as the density of eavesdroppers increases, the average utility per SU decreases. This is due to the fact that as the density of eavesdropping increases, the probability of secure transmission decreases. As expected, the optimal centralized algorithm with full information outperformed the decentralized algorithms. As the decentralized algorithms achieved near-optimal performances, the ICBR again outperformed the DLO algorithm. In the worst case, the former was 4% less than the optimal value while the latter was 24.5% less.

In summary, Figures 3.3 to 3.6 clearly show that the ICBR algorithm was able to provide solid results without the need for a centralized BS to perform the optimization. The results of the DLO algorithm show that the lack of communication between SUs drastically affects the overall network performance.

CHAPTER 4

SMALL CELL NETWORK SECURITY

In this chapter, we switch the topic and discuss the security of small cell networks. As introduced in Section 1.3, small cell networks were presented as a solution to the increasing demand in mobile services. Like most other wireless technologies, small cell networks are susceptible to threats, and therefore security measures and remedies should be advised. In particular, we study, in this chapter, how the potential presence of eavesdroppers and/or jammers may affect the deployment of SCBSs in small cell networks.

We consider that the network operator needs to optimally place the SCBSs in order to boost the efficiency and secrecy of the mobile user transmissions in the presence of security threats. These security threats, such as eavesdropping and jamming [48], are common in military scenarios, and accommodating for their presence is a must when deploying SCBSs for military use. Also, before deploying the SCBSs in cities, the government can provide the network operator with the names of streets and areas that are high-risk and are known for previous malicious network activity (such as hackers, jamming groups, eavesdroppers, etc.). These threats can also be considered in many other scenarios and for different applications, such as securely placing wireless access points in large schools, malls, or other businesses.

The chapter is organized as follows: in Section 4.1, we study a general attack scenario and introduce the general problem. In Section 4.2, we provide the proposed solution for an eavesdropping attack while in Section 4.3, we propose a solution for a jamming attack. Finally, Section 4.4 considers a combination of both aforementioned attacks.

4.1 A General Attack Scenario

Consider a wireless heterogeneous network that is represented by a convex polygon $\mathcal{Q}$. A continuum of wireless users is scattered over the whole area with a density function $\psi : \mathcal{Q} \rightarrow \mathbb{R}^+$. To serve these users, a set $\mathcal{B} = \{b_1, b_2, \cdots, b_n\} \subset \mathcal{Q}^n$ of N small cell base stations (SCBSs)[1] is deployed over $\mathcal{Q}$. A power-law path loss model with exponent μ is considered as the channel model. That is, a signal sent from the origin experiences a gain of $\kappa(1 + d^2)^{-\mu/2}$ at a distance d, with μ the pathloss exponent and κ the pathloss constant. This model is generally used in the study of spatial SINR problems [24].

The deployment of SCBSs in a heterogeneous network considerably affects the performance of all users, and thus it is critical to optimally place these SCBSs. The challenges of optimally deploying SCBSs are exacerbated by the presence of potential security threats at different locations in the network. Under such potential security threats, random or traditional non-secure placement techniques are no longer effective as they allow eavesdroppers to wiretap the transmitted messages, thus breaching the confidentiality of the network. Also, the jammer's signal will decrease the network SINR, compromising the network's availability. The placement problem becomes more challenging when different attack types and scenarios are considered. Each attack type should be handled differently and uniquely in order to minimize its threat to the overall well-being of the network. In this work, we consider the following most common types of attacks: an eavesdropping attack, a jamming attack, and finally a simultaneous jamming and eavesdropping attack.

First, we consider a general attack scenario in which the users are facing security threats and the SCBSs need to be placed in order to minimize the effects of the attacks faced. In our case, the network operator is interested in improving the social welfare of the network by maintaining secure high-gain channels between the users and their serving SCBSs. Accordingly, each user $q \in \mathcal{Q}$ must be assigned a suitable utility function f that captures both the security and the quality of the channel. In general, a user q will connect to the SCBS b_i that maximizes its utility. Hereinafter, we restrict f to be a function of $||q - b_i||$, the distance separating the user q from its serving SCBS

[1] This set can also encompass macrocell base stations.

b_i, although the proposed approach can accommodate other forms for the utility function as well. This class of utilities captures the relative distance between users and the SCBS and covers a large variety of applications such as: placement problems, consensus, and maximum coverage problems [49]. The network operator's problem is to choose the locations of the SCBSs such that the collective social welfare of all users, i.e. the integral of f over the whole network's area $\mathcal{Q}$, is maximized. Thus, the optimal placement problem can be formally written as:

$$\max_{B \in \mathcal{Q}^n} \mathcal{X}(B), \tag{4.1}$$

with

$$\mathcal{X}(B) = \int_{\mathcal{Q}} \max_{i \in \{1,\cdots,n\}} f(||q - b_i||)\psi(q)dq. \tag{4.2}$$

The problem formulated in (4.1) describes the general problem and covers all the attacks considered in this work. $\mathcal{X}(B)$ given in (4.2) is changed to accommodate the attack scenario.

4.2 Eavesdropping Attacks

In this section, we investigate the case where the potential security threats stem from eavesdropping. Eavesdroppers are passive devices that can decode the user messages, thus threatening the confidentiality of the transmitted information. First, we discuss the eavesdropper model, and then provide our solution approach.

4.2.1 Eavesdropper Model

In the considered network, a number of eavesdroppers are assumed to be scattered over a circular area of center $\mathcal{O}$ and radius r. We assume that their exact positions are unknown to the network operator and the users. Here, unlike the assumptions made in Chapter 3, the users and network operator have no information about the densities of eavesdroppers. An example of the SCBS placement problem is given in Figure 4.1.

As we have already discussed in 3.1.2, physical layer (PHY) security techniques [9] are extensively used in many eavesdropping related problems. Section 3.1.2 introduced the probability of secure transmission and it was given

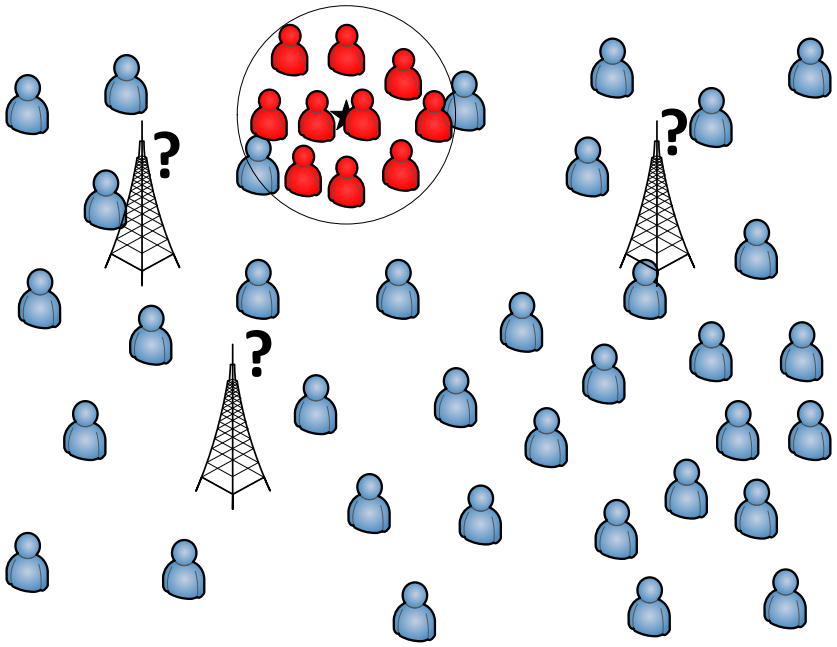

Figure 4.1: Placing SCBSs in the presence of eavesdroppers.

in (3.1). We notice, from (3.1), that obtaining the exact value of this probability requires additional information about the density and distribution of eavesdroppers. As this information is not available here, it is impossible for the network operator or for the user to compute the exact probability.

Nevertheless, a user can always know whether its probability of secure transmission is 1 or less than 1 without computing the exact value. This is solely determined by finding the distances between the user, the serving SCBS, and the region in which eavesdroppers are located. Accordingly, we define a transmission to be secure if and only if the probability of secure transmission is 1. In this chapter, we say that a user is "secure" if its transmission is secure.

4.2.2 The Reward Function

Against such eavesdropping attacks, the network operator aims to place the SCBSs in the network in order to provide secure users with better QoS guarantees. Inherently, the SCBSs need to be closer to the secure users rather than the other non-secure users. That is the case since, as users are in-

terested in message confidentiality, a non-secure transmission is worthless. Thus, secure transmissions should be served better.

Accordingly, to solve this problem we direct our attention to secure users and minimize the distance separating them from their serving SCBS. This translates into the following: the SCBSs should give more priority to users away from the region that is susceptible to eavesdropping and less priority to users near the region that is susceptible to eavesdropping. We achieve this by assigning an artificial density reward function ϕ^E to every user in the network. The reward function represents the priority of each user as perceived by the SCBSs. A higher priority means that a user is more valuable for the SCBSs as it is in a more secure location. Below, we introduce two types of reward functions.

The linear reward

Users inside the region that is susceptible to eavesdropping can never communicate with the SCBS with probability 1 and hence a reward of 0 is assigned to them. Users farther away from this insecure region are more probable to securely communicate with the SCBS. Hence, as users gradually move away from the insecure region, they are given higher priorities by the SCBSs. This is reflected by assigning user q a positive reward, which is $||q-O||-r$, where $||q-O||$ is the distance between the user q and $\mathcal{O}$, the center of eavesdropping.

Equation (4.3) and Figure 4.2 summarize the linear reward function.

$$\phi_1^E(q) = \begin{cases} 0 & \text{when } ||q-O|| \leqslant r, \\ ||q-O|| - r & \text{else.} \end{cases} \tag{4.3}$$

The square reward

In a similar manner, we introduce a square distance reward density function. Using the same analysis, users inside the insecure region are assigned a reward of 0. Higher reward values are assigned to users farther away and this is reflected by assigning user q a positive reward, which is $(||q-O||-r)^2$, where $||q-O||$ is the distance between the user q and $\mathcal{O}$, the center of

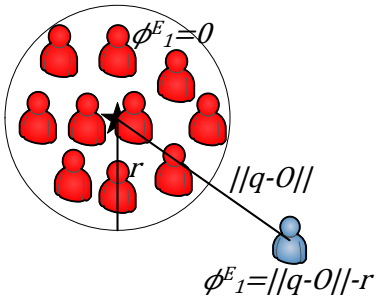

Figure 4.2: The linear reward function ϕ_1^E.

eavesdropping.

Formally, the square reward function is given by:

$$\phi_2^E(q) = \begin{cases} 0 & \text{when } ||q-O|| \leqslant r, \\ (||q-O|| - r)^2 & \text{else.} \end{cases} \tag{4.4}$$

4.2.3 Proposed Solution Approach

The eavesdropping problem is a special case of the general attack scenario presented in Section 4.1. The next step is to define the utility function f. Users are interested in secure transmissions while also maintaining a desirable quality of service, as quantified by the channel quality. Both are achieved by being as close to the SCBS as possible. Therefore, we define $f(q) = -||q-b_i||^2$ where b_i is the SCBS serving user q. The priority of each user is bundled with its density, and hence $\mathcal{X}(B)$ becomes:

$$\begin{aligned} \mathcal{X}(B) &= \int_{\mathcal{Q}} \max_{i\in\{1,\cdots,n\}} -||q-b_i||^2 \psi(q)\phi^E(q)dq \\ &= -\int_{\mathcal{Q}} \min_{i\in\{1,\cdots,n\}} ||q-b_i||^2 \psi(q)\phi^E(q)dq, \end{aligned} \tag{4.5}$$

where ϕ^E can be either the linear reward ϕ_1^E or the square reward ϕ_2^E.

Therefore, the problem of optimal placement of SCBSs in a wireless network with potential eavesdropping threat is given by (4.1) with $\mathcal{X}(B)$ given in (4.5). To study the properties of $\mathcal{X}(B)$, we state the following lemma:

Lemma 4.1. *If f is concave, then $\mathcal{X}(B)$ is concave in b.*

Proof. For a fixed q, the map $b \mapsto f(||q-b||)\phi^E(q)\psi(q)$ is concave, and the integral with respect to q will also be concave [47]. □

Using Lemma 4.1, we can see that $\mathcal{X}(B)$ is concave in b_i for all i and thus to find the optimal locations of SCBSs, it is necessary and sufficient to look at the configurations in which the derivative is zero. To evaluate the integral in (4.5) and to facilitate the derivation, we use the concept of Voronoi partitions defined as follows [50]:

Definition 4.1. *Given a set* $\mathcal{Q} \subset \mathbb{R}^2$ *and a set* $\mathcal{B} = \{b_1, b_1, \cdots, b_n\} \subset \mathcal{Q}^n$*, the* Voronoi partition *of* $\mathcal{Q}$ *generated by* $\mathcal{B}$ *is the collection of sets* $\{V_1(B), \cdots, V_n(B)\}$ *defined by:* $V_i(B) = \{q \in \mathcal{Q} | \, ||q-b_i|| \leqslant ||q-b_j|| \forall b_j \in \mathcal{B}\}$.

Using Definition 4.1, the integral in (4.5) becomes:

$$\mathcal{X}(B) = -\sum_{i=1}^{n} \int_{V_i(B)} ||q-b_i||^2 \psi(q)\phi^E(q)dq. \tag{4.6}$$

Deriving $\mathcal{X}(B)$ with respect to b_i gives:

$$\begin{aligned} \frac{\partial \mathcal{X}(B)}{\partial b_i} &= 2\int_{V_i(B)} (q-b_i)\psi(q)\phi^E(q)dq \\ &= 2M_{V_i(B)}(C_{V_i(B)} - b_i), \end{aligned} \tag{4.7}$$

where $M_{V_i(B)} = \int_{V_i(B)} \psi(q)\phi^E(q)dq$ is the mass of the area $V_i(B)$ with respect to the joint reward-density function $\psi\phi^E$ and $C_{V_i(B)} = \frac{\int_{V_i(B)} q\psi(q)\phi^E(q)dq}{M_{V_i(B)}}$ is the center of mass of $V_i(B)$ weighted according to $\psi\phi^E$. So, to find the maximizing solution, we can use the following law: $b_i = C_{V_i(B)}$.

We now present the optimal placement algorithm which we use to arrive at the optimizing solution. First, we start with random SCBS positions $\mathcal{B}_0 \subset \mathcal{Q}^n$. Then, for each SCBS b_i, the maximizing law $b_i = C_{V_i(B)}$ is applied to arrive at the new positions. $V_i(B)$ is obtained at this stage by holding the positions of all other SCBSs fixed. Finally, after calculating all the new positions, the network operator computes the new Voronoi partition $V_i(B)$ for each b_i and repeats the previous step until convergence. We note that, although this algorithm is carried out by the network operator, it is actually distributed by nature. Algorithm 4.1 gives the details of the optimal placement algorithm.

Algorithm 4.1 Proposed Optimal Placement Algorithm

procedure STAGE 1 ▷ Initialization
    Start with a random SCBS positions $\mathcal{B}_0 \subset \mathcal{Q}^n$.
end procedure

procedure STAGE 2 ▷ Optimal Placement Update
    repeat
    For all $b_i \in \mathcal{B}_0$, each b_i assumes all other b_j's are fixed and finds its Voronoi set $V_i(B)$.
    The new positions are obtained using $b_i = C_{V_i(B)}$.
    Each b_i updates its position in $\mathcal{B}_0$.
    until $\mathcal{B}_0$ converges.
end procedure

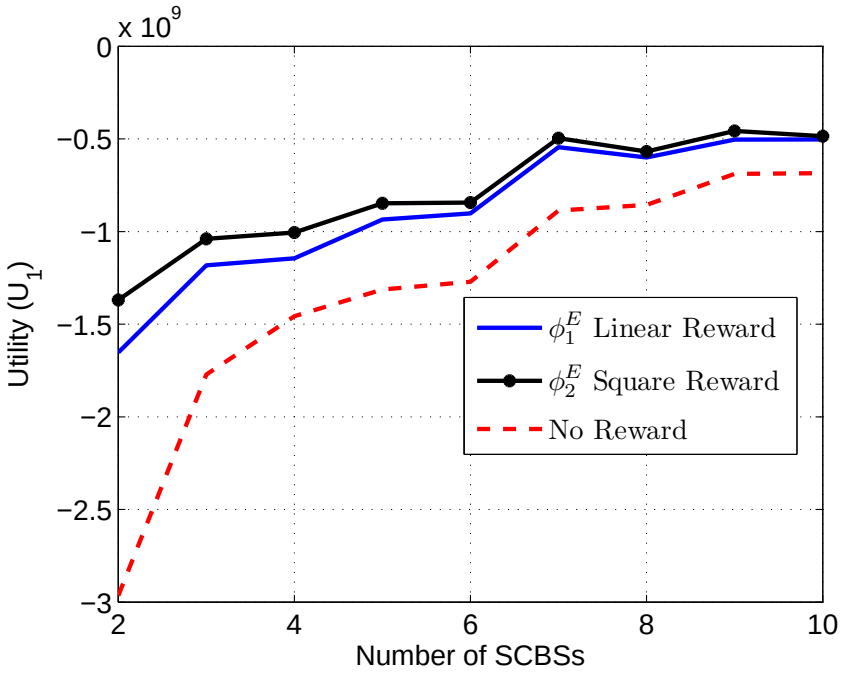

Figure 4.3: Average utility of users U_1 as the number of SCBSs varies.

Remark 4.1. *This proposed algorithm can be easily shown to be a special case of the class of discrete-time spatially-distributed algorithms for coverage control introduced in [50]. Consequently, as per [50], it is guaranteed that the proposed algorithm will converge to the unique optimal solution.*

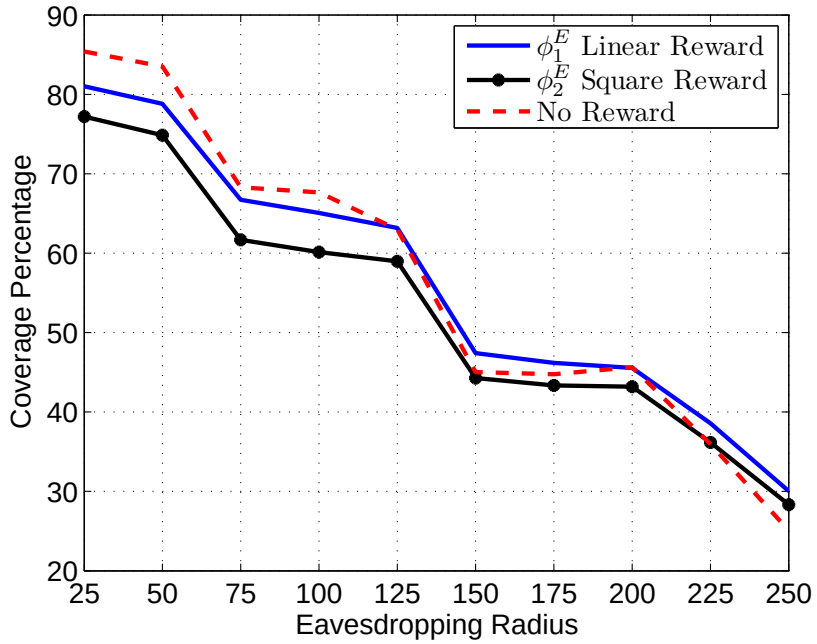

Figure 4.4: Percentage of users covered versus the eavesdropping radius.

4.2.4 Simulation Results and Analysis

We now simulate the presented optimal placement algorithm and study at its performance. We consider $\mathcal{Q}$ to be a 500 m$\times$500 m square area with the wireless users uniformly distributed over it. Eavesdroppers are spread over a disk with known center $\mathcal{O}$ and radius r. No other information is available to the network operator about the eavesdroppers' locations or densities. All statistical results are averaged over multiple random runs for different locations of eavesdroppers and starting points of the algorithm.

We compare the performance of the different reward functions against the base case with no reward for the utility function U_1 given by:

$$U_1 = \int_{\mathcal{Q}} \max_{i\in\{1,\cdots,n\}} -||q - b_i||^2 1_{\{p=1\}},$$

with p the probability of secure transmission. U_1 represents the negative square distance of secure users, i.e. users who can securely communicate with the SCBS. The no reward case places the SCBSs optimally without regarding the eavesdropping threat, similar to [24].

Figure 4.3 shows the variation in utility (U_1) as the number of SCBSs increases for a constant eavesdropping radius $r = 125$ m. In this figure,

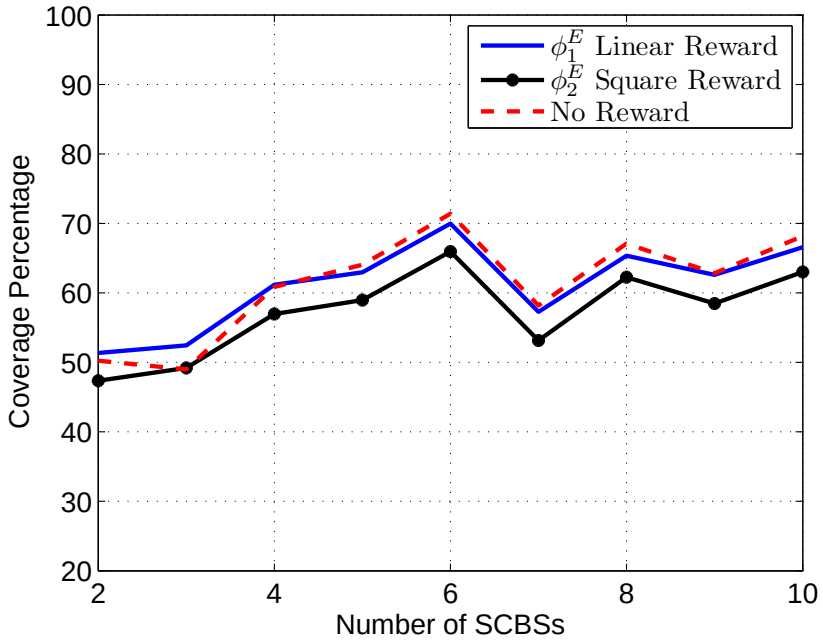

Figure 4.5: Percentage of users covered versus the number of SCBSs.

we can see that the proposed algorithm, when used with square and linear rewards, yields up to 53.9% and 44.3% improvement in the overall utility U_1 at $n = 2$ over the algorithm with no reward respectively. Also, as the number of SCBSs increases for a constant eavesdropping radius, the utility generally increases until it finally saturates. This is due to the fact that the relative distance between users and SCBSs is decreasing.

In Figure 4.4, we further evaluate the performance of the proposed approach using the "coverage percentage" as a metric, as the eavesdropping radius varies. The coverage percentage is defined as the percentage of secure users, users that can securely communicate with their serving SCBS. Figure 4.4 clearly shows that the algorithm with no reward covers more users for a lower eavesdropping radius. As the eavesdropping radius increases, linear reward and square reward start performing better. This is due to the fact that the linear and square rewards penalize the non-secure users and reward the farther away secure users. Here, the coverage percentage obtained by the algorithm with linear reward was within 95% to 120% of the no reward case while the square reward was within 89% to 113%.

In Figure 4.5, we further show that as the number of SCBSs increases for a constant eavesdropping radius, 125 m in this case, the percentage area

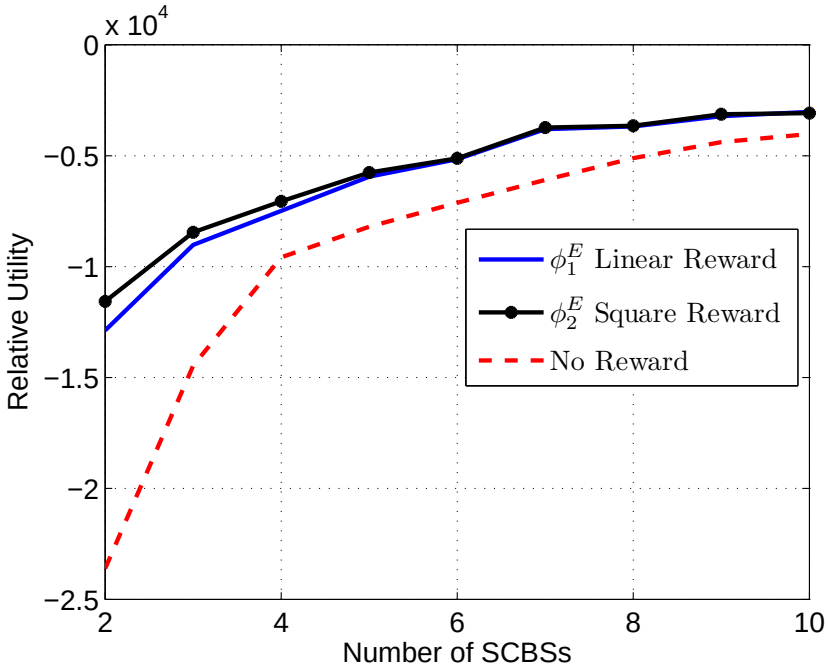

Figure 4.6: Average utility versus the number of SCBSs.

covered generally increases. This is due to the fact that with more available SCBSs, users are closer to the SCBSs and hence it is more probable for them to be secure. Also, the coverage percentage obtained by the algorithm with linear reward was within 98% to 107% of the no reward case while the square reward was within 91% to 100%.

Figure 4.6 shows the relative utility as the number of SCBSs increases. The relative utility is defined as the ratio of the average utility U_1 to the area covered. In other words, it combines both aspects presented in Figure 4.3 and Figure 4.5 as it represents the utility per unit area. Figure 4.6 shows that the algorithm with the square and linear reward functions was able to overcome the effect of eavesdropping and provide the users with higher relative utilities. The square and linear rewards yield up to 51.0% and 45.5% improvement in the relative utility at $n = 2$ over the algorithm with no reward respectively. As the number of SCBSs increases, the gap between the rewarded and non-rewarded plots decreases. This is due to the fact that adding more SCBSs makes the users closer to their serving SCBS, thus rendering the reward functions less influential.

Clearly, by analyzing Figures 4.3 to 4.6, we can conclude that using either the linear reward ϕ_1^E or the square reward ϕ_2^E gives better average and relative

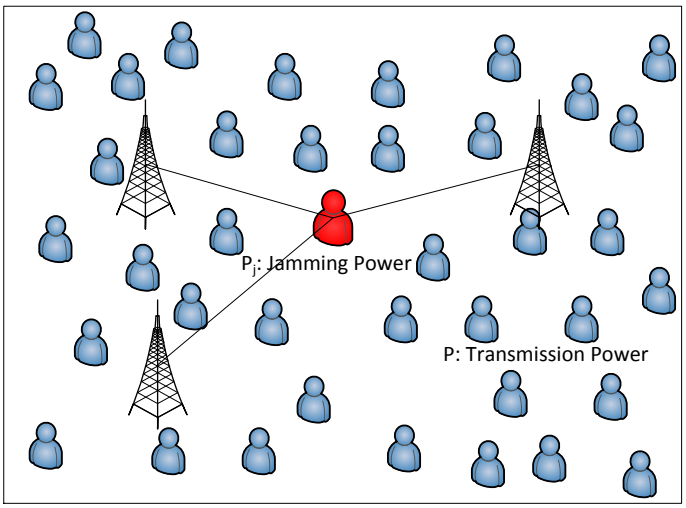

Figure 4.7: A jammer jamming 3 SCBSs.

utilities than the no reward case. The network operator may opt to choose the linear ϕ_1^E over the square ϕ_2^E as it provides better coverage percentages with similar relative utility results.

4.3 Jamming Attacks

In this section, we introduce the jamming problem. First, we discuss the jammer model and then we provide our solution approach.

4.3.1 Jammer Model

In addition to the N SCBSs, a jammer, with a constant jamming power P_j and a linear jamming cost coefficient c_j, exists in the network. As jamming with high power can lead to immense energy expenditures, a constant cost c_j is added to capture the price of jamming. The jammer's location information can be obtained by the network operator by monitoring the network activity and using known signal processing techniques [33]. Figure 4.7 shows a jammer acting in a network with three SCBSs.

In the presence of a jammer, the network operator aims to place the SCBSs in order to increase the overall downlink SINR of the network. Without loss of generality, we study the case in which all the SCBSs are using the same

frequency band. The overall SINR is then given by:

$$\text{SINR} = \sum_{i=1}^{n} \int_{V_i(B)} \frac{P\kappa \left(1 + ||q - b_i||^2\right)^{-\mu/2}}{I(b_i) + P_j\kappa \left(1 + ||j - b_i||^2\right)^{-\mu/2} + \sigma^2} \psi(q)\, dq, \tag{4.8}$$

where $I(b_i)$ is the interference experienced at the SCBS b_i by all wireless users in the network when using the same frequency band, and it is given by:

$$I(b_i) = \int_{\mathcal{Q}} \theta \cdot P\kappa \left(1 + ||x - b_i||^2\right)^{-\mu/2} dx, \tag{4.9}$$

where $\theta \in [0, 1]$ represents the fraction of users that are currently utilizing the downlink channel. Certainly, our approach can accommodate the presence of multiple jammers and can be easily extended for other frequency sharing techniques.

First, we investigate the behavior of the jammer. A user's transmission is either safe or jammed (i.e. not safe). We define a transmission to be safe when the power of the signal received at the SCBS by the user is higher than that received by the jammer. In other words, a user's transmission is safe when

$$P\kappa(1 + d^2)^{-\mu/2} \geqslant P_j\kappa(1 + d_j^2)^{-\mu/2}, \tag{4.10}$$

where d is the distance between the user and its serving SCBS and d_j is that between the jammer and the same SCBS. We can directly change (4.10) to

$$d^2 \leqslant \beta(d_j^2 + 1) - 1, \tag{4.11}$$

with $\beta = \left(\frac{P_j}{P}\right)^{\frac{-2}{\mu}}$.

The jammer's main objective is to jam the maximum possible area. Intuitively, this is the same as minimizing the safe area or equivalently, minimizing β. At the same time, the jammer incurs some costs for using the power and hence the problem becomes:

$$\min_{P_j \geqslant 0} \left(\frac{P_j}{P}\right)^{-2/\mu} + c_j P_j. \tag{4.12}$$

Lemma 4.2. *The function to be minimized in (4.12) is convex in P_j and the*

optimal value P_j^* is given by:

$$P_j^* = \left(\frac{\mu}{2} c_j P^{\frac{2}{\mu}}\right)^{\mu/(\mu+2)}. \tag{4.13}$$

Proof. The second derivative proves convexity. Applying the theory of unconstrained convex optimization leads to the solution in (4.13). □

From (4.13), as the jamming cost c_j increases, the optimal jamming power P_j^* decreases. Similarly, P_j^* also decreases with increase in P, the users' sending power.

4.3.2 The Reward Function

In order to maximize the SINR of the network, we introduce an approximate problem that simplifies the placement problem. We look at (4.11) again and we rewrite it as:

$$d^2 \leqslant \beta d_j^2 + (\beta - 1). \tag{4.14}$$

The locations of the SCBSs affect the values of d and d_j. According to (4.14), the SCBSs seek to minimize d^2 and maximize d_j^2 in order to enhance the performance of wireless users. Recall that d is the distance between the user and the serving SCBS while d_j is the distance between the SCBS and the jammer. Hence, in order to minimize d^2, the users connect to the nearest SCBS and the SCBS minimizes the distance with the wireless users. To maximize d_j^2, the SCBS should be farther away from the jammer.

Thus, in summary, the SCBSs have to minimize the distance separating them from the users without being too close to the jammer. To address this problem, we introduce a jamming threshold ϵ. The jamming threshold is the value beyond which the SCBS considers the jammer as ineffective. So, if $P_j(1 + d_j^2)^{-\frac{\mu}{2}} < \epsilon$, jamming is ineffective. We say that an SCBS is inside the effective area if it is within a distance R^* from the jammer, where:

$$R^* = \left(\left(\frac{P_j}{\epsilon}\right)^{-2/\mu} - 1\right)^{1/2}. \tag{4.15}$$

In order to prevent the SCBSs from residing inside the effective area, we add an artificial reward function ϕ^J for the wireless users in the network. To

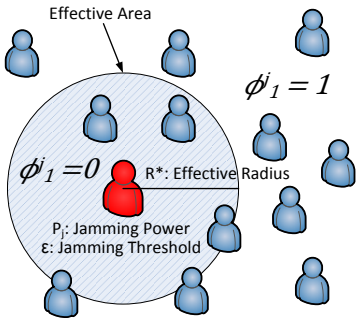

Figure 4.8: The reward function ϕ_1^J.

ensure that the SCBS will be placed farther away from the jammer, we set the reward $\phi_1^J(q)$ of user q to:

$$\phi_1^J(q) = \begin{cases} 0 & \text{when } ||q-j|| \leqslant R^*, \\ 1 & \text{else,} \end{cases} \tag{4.16}$$

where j is the location of the jammer. We will also consider another reward function $\phi_2^J(q)$ and it is given by

$$\phi_2^J(q) = \begin{cases} ||q-j||^2 & \text{when } ||q-j|| \leqslant R^*, \\ (R^*)^2 & \text{else.} \end{cases} \tag{4.17}$$

Figure 4.8 shows the reward function ϕ_1^J with a network jammer.

4.3.3 Solution Approach

Consequently, the problem to be solved is to maximize $\mathcal{X}(B)$ over the possible locations, where:

$$\begin{aligned} \mathcal{X}(B) &= \int_{\mathcal{Q}} \max_{i\in\{1,\cdots,n\}} -||q-b_i||^2 \phi^J(q)\psi(q)dq \\ &= -\int_{\mathcal{Q}} \min_{i\in\{1,\cdots,n\}} ||q-b_i||^2 \phi^J(q)\psi(q)dq \\ &= -\sum_{i=1}^{n} \int_{V_i(B)} ||q-b_i||^2 \phi^J(q)\psi(q)dq, \end{aligned} \tag{4.18}$$

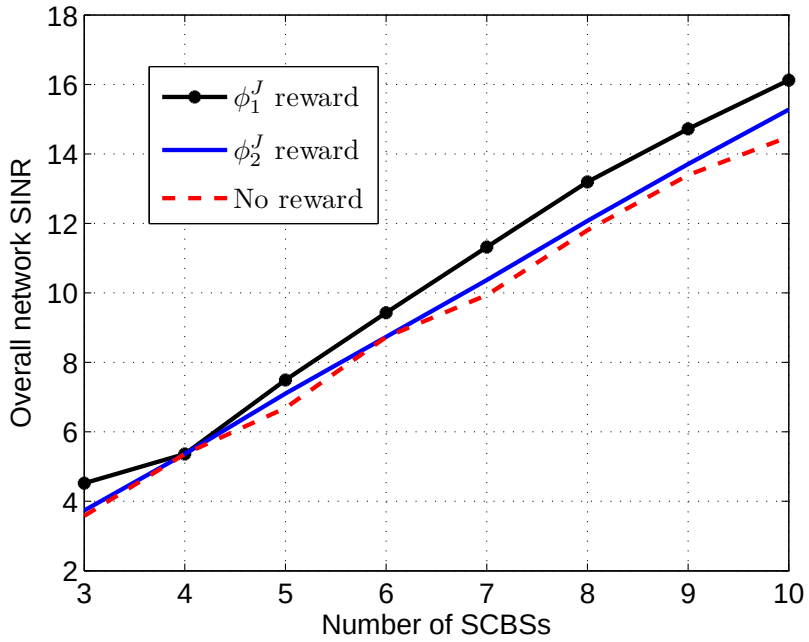

Figure 4.9: Overall network SINR versus the number of SCBSs.

with $V_i(B)$ the Voronoi partition of b_i generated by the set of positions B, defined in Definition 4.1, and $\phi^J(q)$ can be either $\phi_1^J(q)$ or $\phi_2^J(q)$. Notice that the problem the SCBSs have to solve is similar to (4.1) in 4.2.3.

Using the same optimal placement algorithm given in Algorithm 4.1, we can solve the problem in (4.18) and obtain the optimal solution for the locations of the SCBSs. The optimal placement algorithm works exactly the same way for the case of the jammer, and its convergence to the optimal solution again holds.

4.3.4 Simulation Results and Analysis

To assess the performance of the optimal placement algorithm against a jammer, we evaluate the overall SINR of the network as per (4.8). Again, we simulate the presented algorithm over a 500 m$\times$500 m square network and the wireless users uniformly distributed over it. The transmission power of users is set to $P = 100$ mW while the jamming cost is fixed to $c_j = 0.5 \times 10^{-4}$, unless otherwise specified. The wireless medium has a pathloss exponent $\mu = 3$ and a noise level $\sigma^2 = 10^{-12}$. We set the jamming threshold $\epsilon = 10^{-3}$. We set the density of the users to $1,000$ users/km^2 (to represent a typical

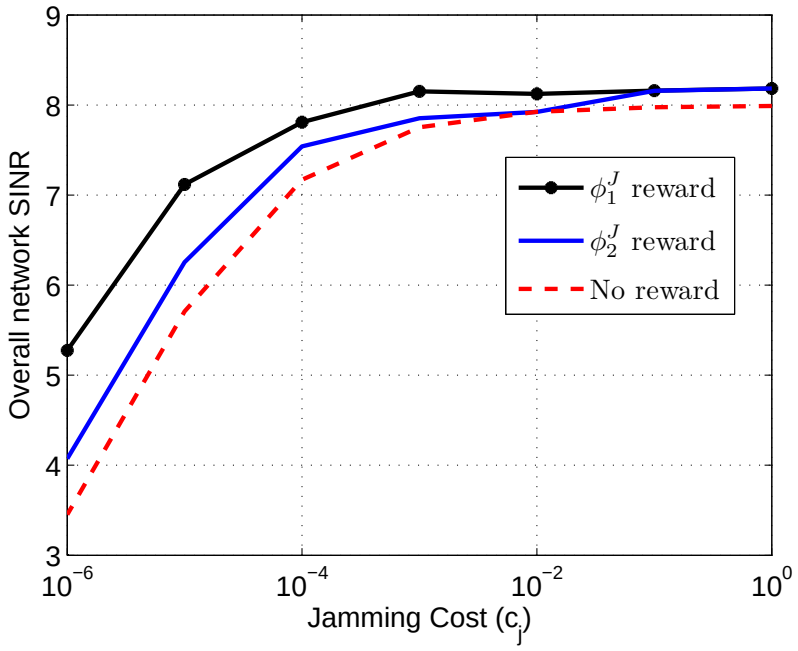

Figure 4.10: Overall network SINR versus the jamming cost c_j.

city) and the network's activity θ to 0.5. This means that half of the users in the network are utilizing the uplink channel at the same time.

Figure 4.9 shows the performance of our approach in terms of the overall SINR given in (4.8). The performance of our algorithm is evaluated when using ϕ_1^J and ϕ_2^J as reward functions in comparison with the base case (i.e. no reward added). Again, the no reward case represents the optimal placement with no regard for the jamming threat. Figure 4.9 shows that as the number of SCBSs increases, the overall SINR of the network increases. This is due to the fact that the users are becoming closer to their serving SCBS. Using the reward function ϕ_1^J provides the highest overall network SINR for different numbers of SCBSs ranging from 3 to 10. It outperforms both the no reward and ϕ_2^J reward for all values of n and provides up to 26.1% increase at $n = 3$ over the no reward scenario. This is the case since it prevents the SCBSs from approaching the jammer in a certain radius, but at the same time, it keeps on minimizing the distance to the users. The reward function ϕ_2^J gives a better performance than the base case overall, but it penalizes less for being near the jammer thus affecting its performance compared to ϕ_1^J.

In Figure 4.10 we show the overall network SINR for all three rewards as the jamming cost c_j increases. We notice that the overall network SINR

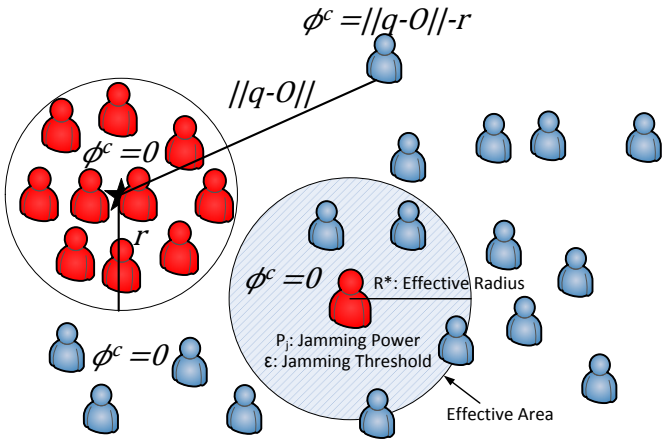

Figure 4.11: The compound reward function ϕ^C.

increases with the increase in c_j. This is the case since increasing c_j decreases the jamming power P_j^* exponentially, thus increasing the SINR. We note that for lower values of c_j, the jamming power is high and the reward functions are able to provide better SINR values and up to 52.8% and 18.0% increase for ϕ_1^J and ϕ_2^J respectively against the no reward at $c_j = 10^{-6}$.

From Figures 4.9 and 4.10, we can clearly see that using the optimal placement algorithm with ϕ_1^J reward function outperforms both the ϕ_2^J and no reward cases.

4.4 Simultaneous Eavesdropping and Jamming

In this section, we consider the case in which both an eavesdropping region and a jammer are present simultaneously in the network. We maintain the same assumptions about the attackers as in the previous sections. In this scenario, the purpose of the network operator is to deploy the SCBSs so as to maximize the uplink SINR of secure users. The jammer's main purpose is to deny the service of the network and not to disrupt the eavesdropping attack. Therefore, to keep both attacks simultaneously effective and to eliminate the jamming effect on the eavesdroppers, we assume that there is no conflict of interest between the jammer and the eavesdroppers.

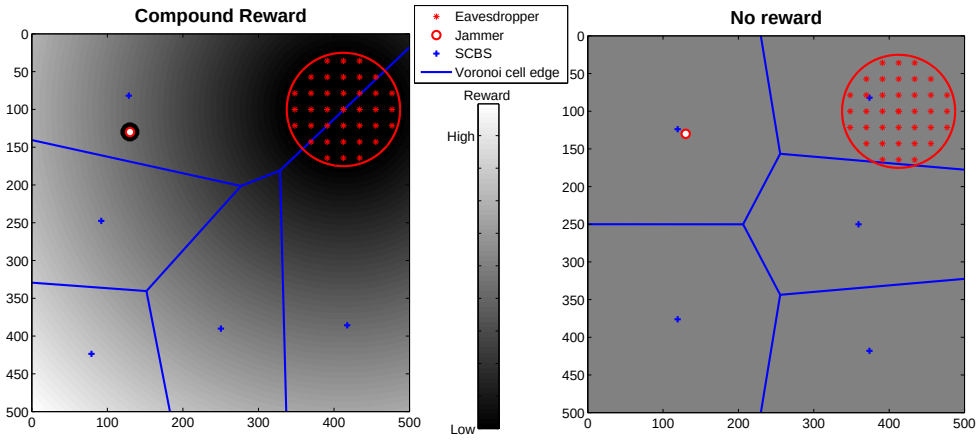

Figure 4.12: The final positions of the SCBSs as given by the optimal placement algorithm with and without the compound reward.

4.4.1 The Reward Function

Based on the previous simulations, we can see that, for the operator, an optimal strategy is to use the reward function ϕ_1^E against eavesdroppers and ϕ_1^J against jammers. Accordingly, we construct the compound reward function $\phi^C(q) = \phi_1^E(q) \times \phi_1^J(q)$ that combines both aspects of the reward functions.

$$\phi^C(q) = \begin{cases} 0 & \text{when } ||q - O|| \leqslant r, \\ 0 & \text{when } ||q - j|| \leqslant R^*, \\ ||q - O|| - r & \text{else.} \end{cases} \tag{4.19}$$

Figure 4.11 shows a network attacked by eavesdroppers and a jammer with the reward function ϕ^C.

4.4.2 Solution Approach and Simulations

Define $\mathcal{X}(B)$ as in (4.5) and (4.18), by

$$\mathcal{X}(B) = -\sum_{i=1}^{n} \int_{V_i(B)} ||q - b_i||^2 \phi^C(q)\psi(q)dq. \tag{4.20}$$

The problem to be solved by the network operator is to place the SCBSs to maximize $\mathcal{X}(B)$ as given by (4.20). This is similar to the general problem given in (4.1). To solve this problem, we use the optimal placement algorithm

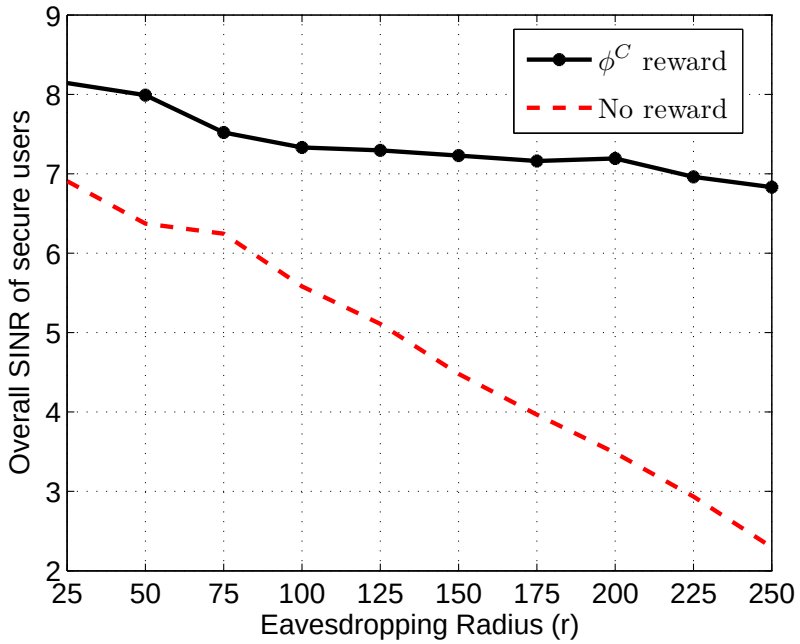

Figure 4.13: Overall SINR of secure users versus the eavesdropping radius.

as given by Algorithm 4.1.

Here, we once again consider a 500 m×500 m square network with uniformly distributed users in the presence of both a jammer and an eavesdropping region (as given in 4.2.4 and 4.3.4). To simulate a simultaneous attack, we need to keep both the jamming and eavesdropping attacks effective. We achieve this by placing the jammer far away from the eavesdroppers. This renders the effect of jamming on the eavesdroppers negligible, and thus it can be neglected. Accordingly, the analysis in 4.2.1 holds. The simulation parameters are the same as those in 4.2.4 and 4.3.4 combined.

Figure 4.12 shows the final positions of the SCBSs as obtained by the optimal placement algorithm with and without the compound reward in a heterogeneous network attacked by a jammer and a set of eavesdroppers. On the one hand, the algorithm with no reward, i.e. the nonsecure placement, deploys one SCBS between the eavesdroppers and another one very close to the jammer. On the other hand, the algorithm with the compound reward penalized users for being near the eavesdropped area and the jammer (as shown by the darker areas). Consequently, the proposed approach was able to place the SCBSs away from the jammer and the eavesdroppers while keeping a structure similar to the non-rewarded case, thus improving the overall

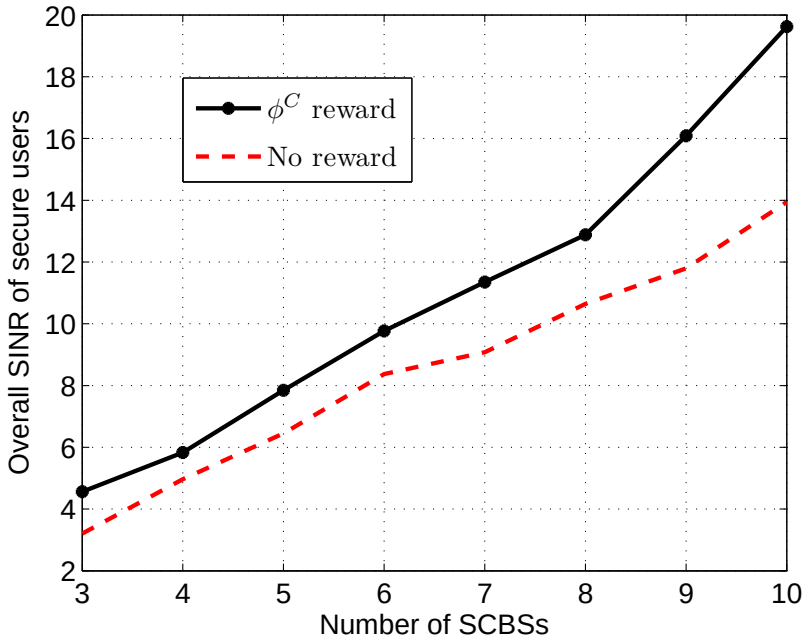

Figure 4.14: Overall SINR of secure users versus the number of SCBSs.

network security.

Figure 4.13 shows that as the eavesdropping radius r increases, the overall network SINR decreases for both with and without the reward function. This is due to the fact that as the eavesdropping radius increases, the percentage of secure users decreases. On the one hand, the no reward suffered from dramatic decreases in the SINR while on the other hand, the reward function was able to contain the damage and provide up to 197% improvement at $r = 250$ m.

In Figure 4.14, we show the SINR of secure users as the number of SCBSs increases. We notice that the overall SINR of secure users increases with the increase in the number of SCBSs. This is due to the fact that the users are becoming closer to their serving SCBS; thus, both the percentage of secure users and their SINR increase. The reward function ϕ^C outperformed the no reward case for all values of n and was able to provide a 42.3% increase in the SINR at $n = 3$.

Figure 4.15 shows the overall SINR of secure users as a function of the jamming cost. As the jamming cost increases, the jamming power decreases and thus the network SINR increases. Again, the ϕ^C reward outperformed the no reward case and was able to provide up to 75.1% better SINR when

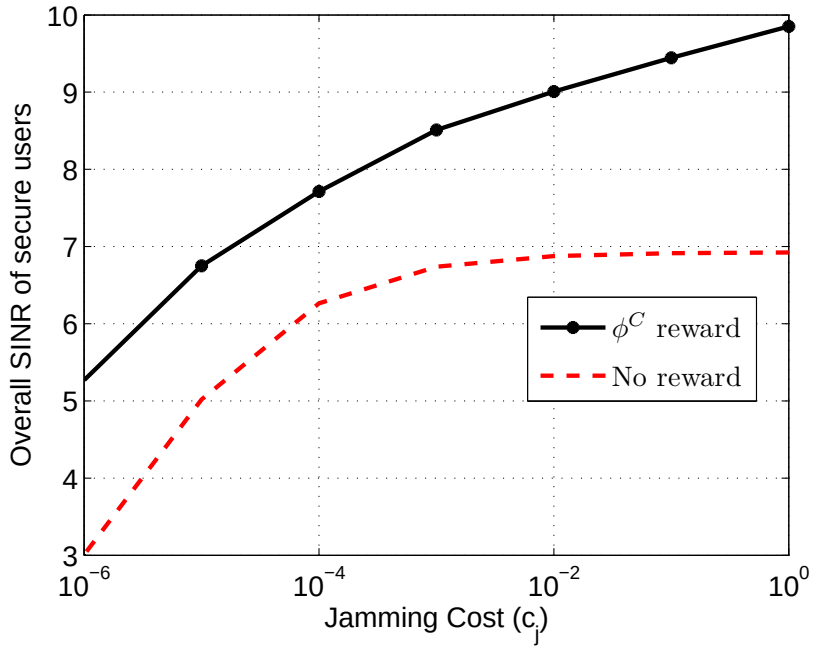

Figure 4.15: Overall SINR of secure users versus the jamming cost (c_j).

$c_j = 10^{-6}$.

Clearly, Figures 4.13 through 4.15 show that the optimal placement algorithm suffered from huge performance degradations under simultaneous jamming and eavesdropping when used with no reward. When used with the ϕ^C reward, it was able to provide significant improvements and, to a great extent, overcome the damage of both eavesdropping and jamming.

CHAPTER 5

CONCLUSIONS

In this thesis, we have investigated the potential security threats in emerging wireless technologies. First, we have analyzed, using game theoretic techniques, the interactions between SUs and eavesdroppers in a cognitive radio network in the presence of multiple PUs. To this extent, we have formulated a game between the SUs and eavesdroppers and analyzed its equilibrium assuming that the SUs have full information about the eavesdroppers. In the proposed game, the objective of the SUs was to maximize their secrecy rates while the objective of eavesdroppers was to minimize the overall secrecy rate of the network by maximizing their eavesdropping capabilities. To solve this game, we have introduced a novel secure channel selection algorithm that enables the SUs and eavesdroppers to take distributed decisions that allow them to reach the equilibrium of the game. Simulation results have shown that the proposed approach yields significant improvements, in terms of the average secrecy rate per SU, when compared to classical spectrum sharing schemes.

Then, we have introduced a novel approach to study how the SUs can mitigate the effect of potential eavesdropping and secure their communications with the base station in a cognitive radio network. The SUs must maintain a threshold level of interference and must protect the PU receivers from their transmissions. Accordingly, we proposed an appropriate utility function for the SUs, and then formulated the problem as a generalized assignment problem. We studied the solution to this problem for three different scenarios depending on the ability of the SUs to communicate and the availability of the SU information at the base station. We introduced a centralized approach and two decentralized approaches that can reach a solution. Simulation results show that the proposed decentralized algorithms were able to provide near-optimal performances with much less information.

Finally, we have studied the problem of optimal placement of SCBSs in

adversarial heterogeneous wireless networks. We considered the following three types of attacks: jamming, eavesdropping and simultaneous jamming and eavesdropping. For each scenario, we equipped each user with the appropriate utility, and then formulated each attack scenario as an optimization problem. Using the proposed optimal placement algorithm, we reached at the optimal locations. Simulation results have shown that the proposed approach yields significant improvements in terms of the overall network performance when compared to classical placement techniques.

5.1 Future Work

For cognitive radio networks, future work can consider jamming attacks in cognitive radio networks and how the SUs can evade them given complete/partial knowledge of attackers. For small cells, future work can consider other attack scenarios, such as multiple eavesdropping and jamming. In addition, other aspects of the problem can be studied such as increasing the network coverage, and adding constraints to the optimization such as a minimum interference and maximum transmission radius.

REFERENCES

[1] Cisco Visual Networking Index, "Global mobile data traffic forecast update, 2010-2015," Cisco white paper, 2011.

[2] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. Cambridge University Press, 2009.

[3] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] T. Q. S. Quek, G. de la Roche, I. Guvenc, and M. Kountouris, *Small Cell Networks: Deployment, PHY Techniques, and Resource Management*. New York, USA: Cambridge University Press, Sept. 2012.

[5] J. G. Andrews, "Seven ways that hetnets are a cellular paradigm shift," *IEEE Communications Magazine*, 2013 (to appear).

[6] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, "Femtocells: Past, present, and future," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 497–508, April 2012.

[7] M. Bennis and S. M. Perlaza, "Decentralized cross-tier interference mitigation in cognitive femtocell networks," in *Proc. IEEE International Conference on Communications (ICC)*, Kioto, Japan, June 2011.

[8] Arbor Networks, "Worldwide infrastructure security report 2012," vol. 8, 2012.

[9] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Secure wireless communications via cooperation," in *Proc. of the IEEE 46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, USA, 2008.

[11] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[12] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. of IEEE INFOCOM*, Shanghai, China, 2011.

[13] Y. Wu and K. R. Liu, "An information secrecy game in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sept. 2011.

[14] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multi-dimensional analysis and assessment," *Mobile Networks and Applications*, vol. 13, no. 5, pp. 516–532, Oct. 2008.

[15] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, New Orleans, Louisiana, USA, 2009.

[16] W. Wang, H. Li, Y. Sun, and Z. Han, "Catchit: detect malicious nodes in collaborative spectrum sensing," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, Honolulu, Hawaii, USA, 2009.

[17] T. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Proc. of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, Singapore, 2008.

[18] J. Suris, L. DaSilva, Z. Han, and A. MacKenzie, "Cooperative game theory for distributed spectrum sharing," in *Proc. of the IEEE International Conference on Communications (ICC)*, Glasgow, Scotland, 2007.

[19] S. Subramani, T. Başar, S. Armour, D. Kaleshi, and Z. Fan, "Noncooperative equilibrium solutions for spectrum access in distributed cognitive radio networks," in *Proc. of the 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Chicago, IL, USA, 2008.

[20] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, April 2008.

[21] Informa Telecoms & Media, "Small cell market status," *SmallCell Forum, whitepaper*, December 2012.

[22] J. Laiho, A. Wacker, and T. Novosad, *Radio network planning and optimisation for UMTS*. Wiley Online Library, 2002.

[23] E. Amaldi, A. Capone, and F. Malucelli, "Planning UMTS base station location: Optimization models with power control and algorithms," *IEEE Transactions on Wireless Communications*, vol. 2, no. 5, Sept. 2003.

[24] E. Altman, A. Kumar, C. Singh, and R. Sundaresan, "Spatial SINR games combining base station placement and mobile association," in *IEEE INFOCOM*, Rio de Janeiro, Brazil, 2009.

[25] O. Arnold, F. Richter, G. Fettweis, and O. Blume, "Power consumption modeling of different base station types in heterogeneous cellular networks," in *Future Network and Mobile Summit, 2010*, Florence, Italy, 2010.

[26] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Communications Letters*, vol. 16, June 2012.

[27] S. Bhattacharya and T. Başar, "Optimal strategies to evade jamming in heterogeneous mobile networks," in *Proceedings of the Workshop on Search and Pursuit-Evasion*, Pittsburgh, PA, USA, 2010.

[28] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security*, 2007.

[29] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, June 2004.

[30] P. Echenique, J. Gomez-Gardenes, and Y. Moreno, "Dynamics of jamming transitions in complex networks," *EPL (Europhysics Letters)*, vol. 71, no. 2, p. 325, 2007.

[31] Y.-M. Huang, M.-Y. Hsieh, H.-C. Chao, S.-H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 400–411, May 2009.

[32] A. Houjeij, W. Saad, and T. Başar, "A game-theoretic view on the physical layer security of cognitive radio networks," in *Proc. 2013 IEEE International Conference on Communications (ICC 2013)*, Budapest, Hungary, June 9-13, 2013 (to appear).

[33] J. Proakis and D. Manolakis, *Digital Signal Processing*. Prentice Hall, 2007.

[34] D. Spill and A. Bittau, "Bluesniff: Eve meets Alice and Bluetooth," in *Proc. of the USENIX Workshop on Offensive Technologies (WOOT)*, Boston, MA, USA, 2007. [Online]. Available: http://www.usenix.org/events/woot07/tech/full_papers/spill/spill_html/

[35] J. Xu and B. Chen, "On secure multi-channel communication systems," in *Proc. of IEEE Military Communications Conference (MILCOM)*, San Diego, CA, USA, 2008.

[36] V. Aggarwal, L. Sankar, A. Calderbank, and H. Poor, "Information secrecy from multiple eavesdroppers in orthogonal relay channels," in *Proc. of IEEE International Symposium on Information Theory*, Seoul, Korea, 2009.

[37] T. Başar and G. Olsder, *Dynamic Noncooperative Game Theory*. SIAM Series in Classics in Applied Mathematics, Philadelphia, January 1999.

[38] D. Fudenberg and D. Levine, *The Theory of Learning in Games*. The MIT press, 1998.

[39] J. Marden, G. Arslan, and J. Shamma, "Joint strategy fictitious play with inertia for potential games," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 208–220, Feb 2009.

[40] Q. Zhu, Z. Yuan, J. B. Song, Z. Han, and T. Başar, "Interference aware routing game for cognitive radio multi-hop networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 2006–2015, November 2012.

[41] D. Stoyan, W. Kendall, J. Mecke, and L. Ruschendorf, *Stochastic Geometry and Its Applications*. Wiley New York, 1987, vol. 2.

[42] D. G. Cattrysse and L. N. Van Wassenhove, "A survey of algorithms for the generalized assignment problem," *European Journal of Operational Research*, vol. 60, no. 3, pp. 260–272, 1992.

[43] F. Facchinei, V. Piccialli, and M. Sciandrone, "Decomposition algorithms for generalized potential games," *Computational Optimization and Applications*, vol. 50, no. 2, pp. 237–262, 2011.

[44] J.-S. Pang, G. Scutari, F. Facchinei, and C. Wang, "Distributed power allocation with rate constraints in Gaussian parallel interference channels," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3471–3489, 2008.

[45] M. L. Fisher, "The Lagrangian relaxation method for solving integer programming problems," *Management Science*, vol. 50, no. 12 supplement, pp. 1861–1871, 2004.

[46] L. A. N. Lorena and M. G. Narciso, "Relaxation heuristics for a generalized assignment problem," *European Journal of Operational Research*, vol. 91, no. 3, pp. 600–610, June 1996.

[47] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[48] R. J. Anderson, *Security Engineering: A guide to building dependable distributed systems*. Wiley, 2010.

[49] S. Martinez, J. Cortes, and F. Bullo, "Motion coordination with distributed information," *IEEE Control Systems*, vol. 27, no. 4, pp. 75–88, Aug. 2007.

[50] J. Cortes, S. Martinez, and F. Bullo, "Spatially-distributed coverage optimization and control with limited-range interactions," arXiv preprint math/0401297, 2004.